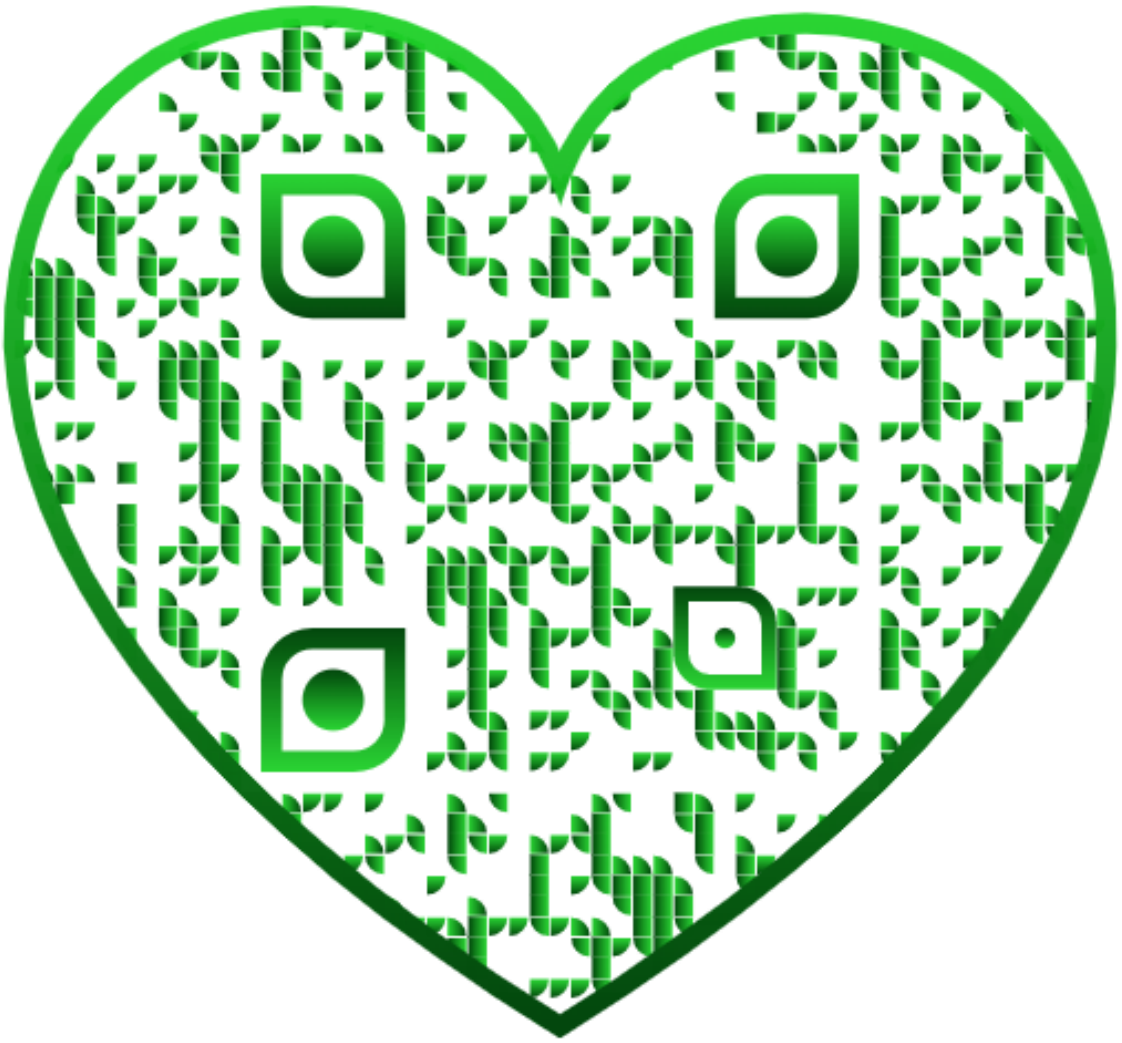
Philippe Herlin

J'ACHÈTE DU BITCOIN

GUIDE PRATIQUE POUR MISER SUR LES NOUVEAUX PLACEMENTS : BITCOIN, ETHEREUM, TOKEN, ICO

EYROLLES

Copyright © 2018 Eyrolles.



Le bitcoin et les cryptomonnaies, mais aussi les mécanismes de levées de fonds proposés par les ICO, constituent autant de placements nouveaux et au potentiel sans équivalent. Mais, aujourd'hui, de nombreuses questions se posent à l'investisseur individuel :

- **Comment fonctionnent le bitcoin et les cryptomonnaies ?**
- **Qu'est-ce que la blockchain ? Une ICO ?**
- **Quel est leur réel potentiel ?**
- **Comment en acheter et les stocker en toute sécurité ?**
- **Quelle est la fiscalité ?**

Philippe Herlin répond à toutes ces questions dans cet ouvrage très pratique. Pédagogue hors pair, il donne tous les conseils pour investir dans les meilleures conditions... et éviter de rater le train.

PHILIPPE HERLIN est économiste, chroniqueur et docteur en économie au Conservatoire national des arts et métiers. Il a publié notamment aux Éditions Eyrolles *Repenser l'économie* (2012), *France, la faillite ?* (2010, 2012), et *Apple, Bitcoin, Paypal, Google : la fin des banques ?* (2015).

www.editions-eyrolles.com

Copyright © 2018 Eyrolles.

J'ACHÈTE DU BITCOIN

Copyright © 2018 Eyrolles.

Groupe Eyrolles
61, bd Saint-Germain
75240 Paris Cedex 05

www.editions-eyrolles.com

Le Groupe Eyrolles ne saurait être tenu pour responsable des éventuels dommages et pertes financières qui pourraient résulter de l'investissement dans le Bitcoin, les autres cryptomonnaies et les ICO. En particulier, tout exemple ou simulation sur l'avenir des cryptomonnaies n'est donné qu'à titre indicatif, et le Groupe Eyrolles ne donne aucune garantie en termes de résultat. Il revient au lecteur d'apprécier par lui-même les risques inhérents à ce type d'investissement.

Les informations contenues dans ce livre sont actualisées à mi-janvier 2018.

En application de la loi du 11 mars 1957, il est interdit de reproduire intégralement ou partiellement le présent ouvrage, sur quelque support que ce soit, sans autorisation de l'éditeur ou du Centre français d'exploitation du droit de copie, 20, rue des Grands-Augustins, 75006 Paris.

© Groupe Eyrolles, 2018
ISBN : 978-2-212-56940-7

Copyright © 2018 Eyrolles.

Philippe Herlin

J'ACHÈTE DU BITCOIN

GUIDE PRATIQUE POUR MISER SUR LES NOUVEAUX PLACEMENTS : BITCOIN, ETHEREUM, TOKEN, ICO

EYROLLES

Copyright © 2018 Eyrolles.

pyright © 2018 Eyrolles.

Sommaire

Introduction 9

1. Comment fonctionne le bitcoin ? 11
   Un réseau décentralisé 11
   L'expérience e-gold 12
   Le modèle Internet 13
   Une monnaie sur Internet ? 14
   L'idée géniale du bitcoin 15
   Le rôle des mineurs 17
   Pas plus de 21 millions de bitcoins 18
   Une invention qui résout plusieurs problèmes à la fois 19
   La signature, un peu de technique 21
   La sécurité du système 22

2. Comment la blockchain réinvente l'économie 25
   Les colored coins 25
   Le smart contract 26
   La smart property 27
   Ubériser Uber ! 28
   Des blockchains… privées 29
   Les DAO 29
   « Code is law » 30

3. Bitcoin, blockchain : un nouveau paradigme 31
   Un potentiel insoupçonnable 31
   La monnaie complémentaire pour tous 32
   Du cash sur Internet 34

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

Économie de la dette versus *économie du cash* 35
Une gouvernance originale 36
La question de la confiance 37

4. Les contre-vérités sur le bitcoin 41
Non, le bitcoin n'est pas anonyme 41
Si, le bitcoin a une valeur intrinsèque 42
Non, le bitcoin n'est pas une pyramide de Ponzi 45
Non, le bitcoin n'est pas une bulle 46
Et si la « bulle du bitcoin » avait en fait déjà éclaté ? 46
Non, le bitcoin ne va pas remplacer les autres monnaies 47
Non, le bitcoin n'a pas besoin d'une banque centrale 48

5. Une histoire mouvementée 49
2009, le lancement 49
2010, la première transaction 49
2011, début d'intérêt des médias 50
2012, naissance de l'intérêt pour la blockchain 50
2013, l'année du bitcoin 51
2014, acceptation par les autorités 52
2015, l'année de la blockchain 52
2016, une progressive montée en puissance 53
2017, l'explosion du cours 53
2018, l'arrivée des investisseurs institutionnels 55

6. Les principales autres cryptomonnaies 57
Comment naissent les cryptomonnaies ? 57
Ethereum 61
Ripple 63
Bitcoin Cash 64
Cardano 64
Litecoin 64
NEM 65
NEO 65
Stellar 65
IOTA 65

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

EOS 65
Dash 66
TRON 66
Monero 67
Bitcoin Gold 67
Les grandes catégories de cryptomonnaies 67

7. Les ICO et les tokens, un nouveau placement 69
ICO, token : les définitions 69
Les avantages de l'ICO pour l'entreprise 71
Les avantages de l'ICO pour l'investisseur 71
L'explosion des ICO lors de l'été 2017 73
Quels sont les risques des ICO ? 75
Les points clés à regarder avant d'investir dans une ICO 77
Deux exemples : iEX.ec et DomRaider 78
2018, l'année où les ICO entrent dans l'âge adulte ? 80
Faut-il investir dans les ICO ? 82
Quelques sites pour s'informer 83

8. La tokenisation de l'économie 85
Des tokens pour des biens existants 85
L'intérêt pour l'investisseur 86
L'intérêt pour le créateur de tokens 86
Les risques 87
Vers une « économie P2P » 88

9. Un bitcoin à 100 000 euros ? Les causes de la hausse du cours 91
Le paiement, première cause de la hausse du cours du bitcoin 91
Le placement, deuxième cause de la hausse du bitcoin 94
La blockchain, troisième cause de la hausse du bitcoin 96
Nous sommes au tout début du phénomène 96
Un cours qui peut atteindre des sommets… 97
La loi de Metcalfe 99
On « découvre » le bitcoin comme on a découvert l'or 100
C'est notre économie qui est une bulle ! 101
Des changements d'échelle à prévoir ? 103

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

10. Les risques associés au bitcoin 105
La concurrence des autres cryptomonnaies 105
Les problèmes de gouvernance et les forks 106
La difficile « scalabilité » du bitcoin 107
Une forte volatilité 109
Le risque d'étouffement par les États 110
L'avis de l'Autorité des marchés financiers 111
L'avertissement d'un acteur du secteur 112

11. Comment acheter des bitcoins ? 113
Les places de marché 113
De nouveaux intermédiaires 115
Obtenir des bitcoins en vendant des biens et des services 116
Obtenir des bitcoins par le minage ? 117
Se méfier des arnaques 118

12. Comment stocker ses bitcoins ? 121
Restez discret 121
Un ordinateur et un antivirus à jour 122
Un wallet *physique* 122
Le Ledger Nano S 124

13. Quelle stratégie d'investissement ? 127
Investir dans les cryptomonnaies et pas ailleurs 127
N'est-il pas trop tard pour en acheter ? 128
Comment diversifier ? 129
Les menaces sur les épargnants du système bancaire « classique » ... 131
Ce qu'en pensent les détenteurs 132

14. La fiscalité 135
Les principes de base 135
On ne déclare qu'en cas de bénéfice 136

15. Des sites pour s'informer 141

Conclusion 143

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

Introduction

Le cours du bitcoin ne cesse de progresser, souvent de façon erratique, et tout le monde en parle, mais il ne faudrait pas que l'arbre cache la forêt : nous assistons à l'émergence d'une nouvelle technologie qui s'apprête à changer en profondeur notre économie. Le bitcoin peut certes améliorer le rendement de notre épargne, mais il va aussi modifier ou bouleverser notre univers professionnel, et plus largement notre façon d'échanger. Il importe donc de bien comprendre le fonctionnement du bitcoin et de la blockchain, d'en dénoncer les contrevérités, de comprendre pourquoi il existe d'autres cryptomonnaies, quelles sont les premières applications concrètes. Nous verrons aussi pourquoi le cours du bitcoin peut autant progresser, mais aussi quels risques il doit affronter, comment en acheter et comment le stocker en toute sécurité. Nous assistons à une aventure monétaire et technologique inédite, faisons en sorte d'en profiter.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

pyright © 2018 Eyrolles.

Comment fonctionne le bitcoin ?

Le terme « bitcoin » vient de *bit* (l'unité d'information la plus simple dans le système binaire, 0 ou 1) et de *coin* (pièce de monnaie en anglais). Avec un b minuscule, bitcoin désigne la monnaie qui circule sur le réseau (ou le *token*, le jeton en français), tandis que Bitcoin avec un B majuscule désigne le protocole, c'est-à-dire la manière donc cela fonctionne. Voyons concrètement comment.

Un réseau décentralisé

Pour comprendre comment fonctionne le bitcoin, il faut se poser la question de savoir pourquoi il existe. Quel est l'objectif poursuivi par la création du bitcoin ? La réponse est qu'il s'agit de créer une monnaie circulant de façon décentralisée sur Internet. Le terme important est « décentralisée ». L'argent électronique existe depuis longtemps, la plupart des euros que nous possédons et utilisons circulent sous cette forme, mais de façon centralisée, c'est-à-dire sous le contrôle de nos banques.

Lorsque nous achetons un produit 10 euros chez un commerçant avec notre carte bancaire, notre compte bancaire est débité de 10 euros et celui du commerçant crédité de la même somme (moins les frais bancaires). Les banques (ou la banque si le commerçant et nous avons la même) sont « l'autorité » qui centralise et valide le paiement, qui

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

conserve la trace de cette transaction, qui arbitre en cas de conflit. On a ici affaire à un système hiérarchisé (les banques au-dessus, et nous les clients).

L'expérience e-gold

Une monnaie électronique circulant de façon centralisée sur Internet a déjà existé, mais cette expérience s'est très mal terminée ; faisons un retour sur l'expérience e-gold. Fondée en 1996 aux États-Unis, cette devise électronique était fondée sur de l'or stocké dans différents pays, la quantité de monnaie en circulation étant couverte à 100 % par de l'or physique. Ainsi, e-gold permettait d'effectuer des virements internationaux et, une fois la transaction réalisée, l'or changeait de propriétaire, même si physiquement les lingots restaient à la même place. Le succès fut au rendez-vous : en 2005, e-gold comptait 3,5 millions d'utilisateurs dans 165 pays et se plaçait deuxième derrière Paypal dans les solutions de transfert d'argent par Internet. Début 2007, les réserves atteignaient 10 tonnes d'or. Mais en avril 2007, la justice américaine accuse la société de blanchiment d'argent, d'absence de licence pour un service de transfert d'argent et d'avoir permis un nombre incalculable d'opérations frauduleuses. L'or est saisi, le système s'écroule et son fondateur, Douglas Jackson, est condamné à de la prison avec sursis.

Cette expérience aura marqué le milieu geek et technophile en démontrant l'impossibilité d'une monnaie électronique centralisée. Les risques sont en effet de deux natures :

- Quelle confiance accorder à l'organisateur ? Le fondateur d'e-gold était honnête, mais comment s'assurer que le dirigeant d'une monnaie de ce type ne parte pas avec la caisse, en l'occurrence les lingots ou, si la monnaie n'est pas fondée sur une contre-valeur, qu'il ne fabrique pas en cachette des unités monétaires

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

pour en donner à ses amis ? Comme si, au Monopoly, celui qui « fait » la banque glissait discrètement des billets à un joueur en particulier, faussant ainsi le jeu ?

- Quelle confiance accorder au pays où sera installée la société gérant cette monnaie ? Le gouvernement ou un juge peuvent décider d'interrompre l'activité et au passage, de ruiner tous les utilisateurs, c'est ce qui s'est passé avec e-gold.

Le modèle Internet

Il fallait passer à un modèle décentralisé. Avec Internet est apparue une façon différente de s'organiser, avec un fonctionnement en réseau plutôt que de façon hiérarchique. Un réseau peut fonctionner de façon hiérarchique, autour d'un nœud central par lequel toutes les informations doivent passer avant d'aller ailleurs (le système de paiement par carte avec les banques), mais il peut aussi être totalement décentralisé, les informations ne devant pas revenir à un serveur unique mais pouvant passer d'un nœud à l'autre, de proche en proche, « de pair à pair », ou en anglais *peer to peer* (abrégé en P2P). Il n'y a plus un nœud centralisant toute l'information, mais un maillage fin laissant passer toutes les informations.

Internet fonctionne de cette façon, il a été conçu pour cela : dans les années 1960 aux États-Unis, le Pentagone s'était rendu compte qu'en cas de guerre nucléaire, le réseau téléphonique deviendrait inutilisable, car les centraux téléphoniques étant situés dans les grandes villes, ils seraient détruits avec elles. Le système de commandement ne pourrait donc plus fonctionner. Les militaires ont demandé à des informaticiens de concevoir un système de transmission décentralisé, dans lequel les « paquets d'informations » pourraient transiter de proche en proche, et même modifier leur chemin en cas de destruction

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

d'une partie du réseau, en allant au plus vite. C'était Arpanet, l'ancêtre d'Internet.

Cette culture décentralisée, non hiérarchique, fait partie de l'« ADN » d'Internet et elle est revendiquée par une partie importante de la communauté des développeurs. Prenons un exemple pour bien comprendre cette idée : pour l'ancestrale encyclopédie Britannica, un comité scientifique peut trancher et dire « pour tel article, nous écrirons telle chose ». Pour Wikipédia, en revanche, il n'existe pas d'autorité centrale possédant ce pouvoir, les contributeurs devant parvenir à un accord. *Idem* dans le milieu du logiciel libre où personne ne peut exiger une fonctionnalité donnée, alors que les patrons de Microsoft ou d'Oracle peuvent imposer une décision. Ce milieu collaboratif et ouvert favorise l'innovation : les imprimantes 3D sont nées dans cet écosystème où les découvertes sont communiquées plutôt que brevetées, où chacun peut lancer une idée, où des outils (forums, gestion de projet) permettent de gérer l'information en toute transparence, sans passer par un filtre hiérarchique.

Une monnaie sur Internet ?

Et pendant longtemps, ce milieu alternatif s'est demandé : « Comment pourrions-nous faire fonctionner une monnaie sur ce modèle ? » – c'est-à-dire sans une banque qui valide et enregistre les transactions. Comment faire circuler une monnaie dans un réseau décentralisé, où il n'existe pas d'autorité, de tiers de confiance, d'arbitre ?

Dans le monde réel, une telle monnaie décentralisée pourrait être mise en œuvre assez facilement, avec un objet que l'on connaît bien : le billet de banque. Un groupe de personnes pourrait tout à fait décider d'imprimer une quantité donnée de billets infalsifiables, détruire les presses pour que personne ne puisse en fabriquer de nouveaux, et se les distribuer. Ensuite le système fonctionne tout seul : quand j'utilise

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

un billet… je ne l'ai plus, et celui qui le reçoit en devient le propriétaire, les débits et les crédits se gèrent naturellement, nul besoin qu'une banque contrôle tous ces mouvements dans ses livres de comptes. Mais sur Internet, ce procédé ne marche pas : la notion de « billet numérique infalsifiable » n'a tout simplement pas de sens, parce que la duplication est consubstantielle au monde numérique ; quand vous envoyez une photo par e-mail en pièce jointe, vous l'avez encore sur votre ordinateur.

L'idée géniale du bitcoin

La question est donc : comment faire circuler sur Internet un objet numérique infalsifiable ? Pour comprendre cela, transposons ce problème dans le monde réel avec un exemple simpliste : nous sommes une vingtaine de personnes dans une salle et nous voulons créer une monnaie. Celle-ci ne sera pas des billets de banque comme on l'a évoqué plus haut, mais de simples feuilles de bristol blanc, que n'importe qui peut acheter dans le commerce, c'est-à-dire « dupliquer ». Avec ce procédé, cela ne pourrait pas fonctionner, personne n'aurait confiance dans une monnaie si aisément falsifiable ! Alors posons-nous la question : que devrions-nous ajouter comme informations pour que le système fonctionne ? Deux éléments :

- Chacun appose sa signature sur les bristols qu'il possède. Et quand j'utilise l'un d'entre eux pour acheter un objet à quelqu'un, celui-ci en devient propriétaire et y appose à son tour sa signature, et ainsi de suite. Si je reçois un bristol sans aucune signature, je sais qu'il n'a aucune valeur. On considère que les signatures sont infalsifiables (ce qui est vrai avec le bitcoin, nous le verrons). Mais cette règle ne suffit pas, un petit groupe d'utilisateurs pourrait acheter des bristols, se les échanger entre eux pour y apposer leurs signatures, puis les remettre dans le circuit… Il faut donc un second élément.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

- L'information concernant tous les bristols en circulation, c'est-à-dire le fait que tel bristol est passé de telle personne à telle autre, etc., est publique, elle est affichée sur un grand tableau visible de tous. Quand je reçois un bristol en paiement d'une transaction, j'y appose ma signature, mais je la mets aussi sur le tableau à la ligne correspondant à ce bristol : je peux ainsi constater que la liste des signatures figurant sur le bristol est identique à celle affichée sur le tableau, c'est donc de la vraie monnaie. Si l'on me propose un bristol avec une suite de signatures que je ne peux pas retrouver sur le tableau, c'est de la fausse monnaie. De cette façon, l'introduction de fausse monnaie est impossible, et les débits/crédits sont parfaitement enregistrés et infalsifiables. C'est ainsi que fonctionne le bitcoin.

Sur Internet, les signatures sont électroniques bien sûr, et elles ne correspondent pas au nom d'une personne, mais à un numéro de compte. D'autre part, le « grand tableau visible de tous » regroupant l'ensemble des transactions est le livre des comptes, la base de données de l'ensemble des transactions, accessible et partagée par l'ensemble des participants (c'est la « blockchain », nous y reviendrons).

Ainsi, chaque bitcoin (ou fraction de bitcoin) est « tracé » depuis le début à partir de ses propriétaires successifs, et cette information est publique. Quand quelqu'un effectue un paiement en bitcoins, on peut remonter ses transactions antérieures pour vérifier qu'il possède effectivement les bitcoins nécessaires ; voilà comment cette monnaie circule. C'est l'idée géniale du bitcoin : la validation des transactions n'est pas réalisée par une instance supérieure, elle l'est par la communauté. C'est comme si en allant sur le site d'une banque, on pouvait voir en direct l'ensemble des virements de compte à compte. C'est bien sûr impossible, nous sommes ici dans le cœur de l'activité bancaire, totalement confidentielle. Pour le bitcoin, cette information

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

est publique[1]. On passe d'un système hiérarchique, vertical, opaque, celui des banques, à un système horizontal, décentralisé, transparent, celui du bitcoin.

Il n'y a pas *un* serveur qui détient toute l'information et dont la coupure ou la prise de contrôle ferait tomber tout le système. Non, l'information (la base de données de l'ensemble des transactions, la blockchain) est publique et partagée entre tous les ordinateurs participant au réseau bitcoin. Le système est donc virtuellement indestructible (à moins de couper Internet sur la planète entière…).

Le rôle des mineurs

Mais qui se charge de vérifier les transactions sur le réseau bitcoin ? Dans notre exemple simplifié, qui vérifie la conformité des bristols avec le « grand tableau visible de tous » ? Il s'agit des « mineurs », tel est leur surnom, un certain nombre de participants du réseau qui se chargent de valider les transactions (c'est-à-dire de vérifier la conformité des signatures et des bitcoins transférés avec les informations de la base de données). Les transactions ne sont pas validées une par une, mais par groupe, on parle de « bloc de transactions » (d'où le terme anglais de *blockchain*). Ils ne font pas ce travail à la main, en cochant des cases devant leur écran, ils font tourner des programmes informatiques 24 heures sur 24 sur des ordinateurs surpuissants dédiés à cela. Les mineurs sont en concurrence et le premier qui réussit à valider un bloc de transactions est récompensé… en bitcoins ! Voilà comment le système fonctionne, il se boucle sur lui-même : ceux qui sont chargés de veiller à son bon fonctionnement ne le font pas par philanthropie, ils sont financièrement intéressés ! Ils investissent dans du matériel informatique, payent des factures élevées d'électricité, mais au final, ils gagnent de l'argent. Ces mineurs creusent, informatiquement

1. On peut voir ces transactions en direct sur le site blockchain.info, par exemple.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

parlant, pour trouver de l'or, de la monnaie numérique. Le réseau Bitcoin est donc parfaitement autonome.

Le bitcoin sera finalement lancé peu de temps après l'effondrement de e-gold en avril 2007 : en octobre 2008 est publié le document de recherche qui explicite son fonctionnement[1] et la première transaction a lieu le 3 janvier 2009.

Pas plus de 21 millions de bitcoins

Les mineurs, qui valident les transactions, sont récompensés en bitcoins, nous venons de le voir. Mais le montant de cette récompense est divisé par deux tous les quatre ans environ. Du 3 janvier 2009 (date de la première transaction) à novembre 2012, la récompense pour la validation d'un bloc de transactions était de 50 bitcoins ; puis elle est passée à 25 ; depuis juillet 2016, elle est descendue à 12,5, et elle tombera à 6,25 en 2021 et ainsi de suite. Ce mécanisme fait partie de l'algorithme, il ne peut pas être modifié et, de la sorte, on peut calculer que le nombre total de bitcoins en circulation ne pourra jamais dépasser 21 millions.

Cette donnée est fondamentale pour bien comprendre la particularité de cette monnaie : le nombre de bitcoins en circulation augmente progressivement (17 millions début 2018), mais il atteindra un plafond de 21 millions qu'il ne dépassera jamais.

Avant de poursuivre, revenons sur les mineurs : quelle sera leur motivation si leur récompense diminue progressivement ? Tout d'abord, ils ne touchent pas que 12,5 bitcoins (aujourd'hui), mais également les frais associés à chaque transaction du bloc. En effet, pour chaque transaction en bitcoins, des frais sont nécessaires (très faibles par rapport aux autres moyens de paiement, mais pas nuls). D'autre part, la valeur des bitcoins augmente avec le temps, de façon certes chaotique,

1. Satoshi Nakamoto, « A Peer-to-Peer Electronic Cash System », 2008.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

mais elle augmente. Les mineurs touchent donc une récompense qui diminue avec les années, mais dont la valeur augmente, ainsi que des frais de transaction, et finalement, ils s'y retrouvent financièrement.

Une précision : le fait que le nombre de bitcoins ne puisse pas dépasser 21 millions ne constitue aucunement une limitation à son développement et à son usage. Il y aura toujours assez de bitcoins pour effectuer des transactions, même si la monnaie connaît un succès grandissant. On parlera alors de millièmes ou de millionièmes de bitcoins ; le bitcoin est actuellement divisible jusqu'à la 8e décimale et ce seuil pourrait être repoussé. Mais entretemps, son cours aura dû augmenter en proportion, afin de satisfaire la demande. C'est comme si l'on déplorait qu'il n'existe que 160 000 tonnes d'or dans le monde (selon les estimations les plus courantes), ce qui ne constitue nullement un problème ; tout dépend du cours de l'or, et s'il devait jouer à l'avenir un rôle monétaire et de placement plus important, son cours grimperait.

On comprend ainsi que le bitcoin est une « monnaie-matière première » une monnaie dont la création monétaire est strictement contrôlée, tendant vers un chiffre fixe, sur un rythme connu à l'avance. On se rapproche beaucoup de l'or dans le principe. On est ici aux antipodes de nos monnaies-papier actuelles, dont la masse enfle au gré des circonstances, soi-disant pour soutenir l'économie, en fait surtout pour permettre encore plus d'accumulation de dettes, publiques et privées. On peut ainsi considérer que le bitcoin, c'est un peu de « l'or numérique ».

Une invention qui résout plusieurs problèmes à la fois

Le bitcoin est-il une monnaie « parfaite » ? On peut le croire lorsque l'on dresse la liste de ses caractéristiques : il est universel, accessible

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

à tous (il suffit d'une connexion Internet), il n'est sous le contrôle d'aucuns État ou entreprise, il est totalement indépendant du système bancaire, autorégulé, sécurisé et sa création monétaire est contrôlée et limitée. Le bitcoin résout également d'un coup tous les problèmes liés à une monnaie-matière première : authenticité des transactions, instantanéité des échanges, divisibilité, homogénéité, stockage. Depuis le début de son existence, le 3 janvier 2009, aucun faux bitcoin n'a circulé, le réseau n'est jamais tombé.

Le bitcoin est au croisement de plusieurs écoles de pensée, de nature très différente :

- les défenseurs du logiciel libre, nous l'avons vu, c'est-à-dire d'un code programme ouvert à tous, dont aucune entreprise ou institution n'est propriétaire, et le refus de la hiérarchie ;
- les penseurs qui soulignent l'importance essentielle des contre-pouvoirs et de la décentralisation des institutions, la méfiance vis-à-vis d'un pouvoir central fort, et auxquels on peut rattacher aujourd'hui les libertariens et les mouvements libertaires ;
- l'école autrichienne, qui défend l'étalon-or et dont plusieurs adeptes actuels voient dans le bitcoin une approche comparable.

D'ailleurs, qui a eu l'idée du bitcoin ? En fait, on ne sait pas. Un dénommé Satoshi Nakamoto s'est fait connaître pour avoir publié le premier un article de recherche sur le sujet, et comme initiateur de la première transaction (le 3 janvier 2009). Mais il s'agit en réalité d'un pseudonyme et, désormais, Satoshi Nakamoto ne communique plus avec personne. Au fond, c'est certainement mieux ainsi : personne ne peut s'approprier la paternité du bitcoin, qui garde dans sa dimension de pur réseau décentralisé, sans qu'une quelconque « personnalité » puisse y jouer un rôle central, ne serait-ce qu'en termes d'image et de notoriété.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

La signature, un peu de technique

Revenons sur la signature électronique[1]. Celle-ci permet deux choses : d'une part authentifier l'émetteur du message, d'autre part contrôler l'intégrité de ce message (vérifier qu'il n'a pas été modifié). La signature électronique n'est devenue possible qu'avec la cryptographie asymétrique, qui est fondée sur l'existence de fonctions mathématiques non inversibles : le message « passe à la moulinette » d'une fonction mathématique, ce nouveau message crypté est envoyé au destinataire, mais il est impossible d'inverser la fonction pour retrouver le message d'origine… à moins de posséder une information particulière tenue secrète. La première fonction est appelée « clé publique », et la seconde, tenue secrète, qui permet de décrypter le message, est appelée « clé privée ». Les deux clés sont liées mathématiquement, de sorte que la clé publique (connue de tous) permet de coder un message, tandis que la clé privée (connue par l'utilisateur seul) permet de le décoder. En somme, une clé privée permet de calculer la clé publique, mais l'inverse est impossible. C'est ainsi que fonctionnent les signatures électroniques, qui existaient bien avant le bitcoin.

Une adresse bitcoin est un compte qui permet de recevoir, de stocker et d'envoyer des bitcoins. On peut la comparer à un numéro de compte bancaire. Une transaction indique le montant versé à une autre adresse bitcoin. Mais cette transaction intègre aussi la transaction précédente, qui elle-même intègre la transaction précédente, etc., jusqu'au début, c'est-à-dire jusqu'à la création des bitcoins nécessaires à la transaction (nous avons dit plus haut que chaque bitcoin est tracé depuis le début). On justifie ainsi que les fonds nécessaires sont bien possédés. Cette transaction circule en clair sur le réseau, le livre des comptes est public et partagé (c'est la blockchain).

1. Pour tous les aspects cryptographiques et mathématiques de la compréhension du bitcoin, on se reportera au *Bitcoin Book* de Pierre Noizat, disponible sur Amazon.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

Il faut bien garder sa clé privée et ne pas la perdre, elle seule permet d'accéder à ses bitcoins et de les dépenser. Une transaction est donc concrètement un message qui comprend le numéro d'identification de la transaction précédente, le montant, la clé publique correspondant à l'adresse bitcoin de l'émetteur, la signature du message par la clé privée de l'émetteur, et l'adresse bitcoin du destinataire. Cette transaction est sécurisée par un système de clés (la clé privée doit correspondre à la clé publique avec laquelle a été créée l'adresse bitcoin en sortie de la transaction précédente). Le couple « adresse bitcoin/clé privée » peut être compris par analogie comme un coffre bancaire muni de sa clé : l'adresse bitcoin représente l'adresse de la salle des coffres et le numéro de coffre, tandis que la clé privée permet d'ouvrir le coffre.

La sécurité du système

La sécurité du bitcoin (le système clé publique/clé privée) repose sur des algorithmes cryptographiques : ECDSA, SHA256. Ces algorithmes sont unanimement considérés comme les plus sûrs, ils sont utilisés dans la banque, l'armée, le renseignement. S'ils étaient « craqués », tous les systèmes électroniques de la planète tomberaient. Voici un exemple d'adresse bitcoin : 175tWpb8K1S7mH4Zx6rewF9wQrcPv245W. Il existe plus de 10^{48} adresses possibles, soit plus d'atomes qu'il y a sur Terre.

D'une façon générale, un système centralisé, dépendant de quelques mots de passe, est fragile, car si le secret est percé, il tombe entièrement (piratages de comptes PlayStation et LinkedIn en 2012, Yahoo ! en 2013, Uber en 2016…). Alors qu'un système décentralisé dans lequel chaque participant est responsable de sa clé privée évite ce risque ; il n'existe tout simplement pas *un* mot de passe qui permettrait de craquer le réseau bitcoin.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

Ensuite, comment vérifier que telle transaction est bien réelle, et non pas un message fabriqué de toutes pièces, ou une tentative d'effectuer le même versement de bitcoins à deux personnes différentes ? C'est là qu'interviennent les mineurs. Lorsqu'une nouvelle transaction est reçue sur le réseau bitcoin, elle n'est pas considérée comme valide tout de suite, elle est incorporée dans ce que l'on appelle un « bloc de transactions ». Un bloc n'est pas une simple liste de transactions, il est lui-même crypté, et il contient également l'empreinte du bloc précédent (c'est-à-dire le bloc crypté, passé à la moulinette d'une fonction non réversible), et ainsi de suite, suivant en cela la logique des transactions elles-mêmes. Tous ces blocs imbriqués rendent impossible la moindre modification d'une transaction sans invalider le bloc et tous les blocs suivants. Ensuite, les mineurs vont se charger de valider ces transactions (les bitcoins versés au destinataire proviennent bien de transactions antérieures, il y a correspondance entre la clé publique et l'adresse bitcoin, etc.), puis d'inscrire le bloc regroupant ces transactions dans la base de données. Au final, les transactions sont liées entre elles dans une chaîne chronologique par un mécanisme sophistiqué de signatures numériques. Puisque aucune transaction ne peut être retranchée ni ajoutée sans avoir été vérifiée par l'ensemble du réseau, la propriété de chaque bitcoin est établie avec certitude.

Le premier mineur à avoir validé ce bloc de transaction touche 12,5 bitcoins, c'est sa « récompense ». Ces bitcoins ne proviennent pas d'une transaction antérieure, il s'agit donc de création monétaire. Une particularité à noter est que la validation d'un bloc se fait à travers une « preuve de calcul » dont le niveau de difficulté est modulé. Résultat, toutes les 10 minutes environ un bloc est validé, et le niveau de difficulté de la preuve de calcul est ajusté tous les 2 016 blocs, soit toutes les 2 semaines, pour rester autour de ces 10 minutes (autrement dit, actuellement, 12,5 bitcoins sont créés toutes les 10 minutes sur le réseau).

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

Quels sont les risques ? Théoriquement, un pool de mineurs qui réunirait au moins 51 % de la puissance de calcul de l'ensemble du réseau pourrait en prendre le contrôle et valider des transactions fictives à son profit (en fait, simplement valider des doubles dépenses, sans même créer des bitcoins). Cependant, outre que des coupe-circuit existent pour parer à une telle éventualité, la somme dépensée pour financer une telle « ferme » de serveurs serait largement supérieure au bénéfice escompté. Le plus rentable, avec une telle puissance de calcul, serait de « miner » (valider les transactions) afin d'empocher les récompenses de 12,5 bitcoins et les commissions de transaction.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

Comment la blockchain réinvente l'économie

Le bitcoin, c'est plus que le bitcoin. Il s'agit d'une monnaie on l'a vu, qui fonctionne grâce à une base de données publique des transactions, la blockchain. Mais cette blockchain peut servir de support à de multiples applications, et c'est sans doute l'aspect le plus révolutionnaire du bitcoin. Voyons-en quelques exemples marquants.

Les *colored coins*

Commençons par un champ d'application connu sous le terme de *colored coin*. Pour comprendre ce mécanisme, prenons une métaphore : un joueur de casino décide de mettre une touche de peinture sur chacun de ses jetons pour voir comment ils vont circuler sur la table de jeu. Transposons sur le réseau bitcoin : des personnes décident de créer une société, elles apportent chacune leur part au capital de cette entreprise en bitcoins et ceux-ci vont être « coloriés » (de façon informatique) avec une couleur précise et ainsi clairement identifiés comme tels. Lorsque cette entreprise distribuera des dividendes, ces bitcoins seront coloriés de la même façon, ce qui permettra d'attester qu'ils proviennent bien d'elle, et ils seront répartis entre les différents actionnaires en fonction de leur part au capital. Ces actionnaires peuvent décider de vendre une partie du capital qu'ils détiennent, ce qui se fera facilement, puisque ces bitcoins sont clairement identifiés grâce à leur « couleur ». Et l'on

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

vient ici tout simplement de créer un marché boursier. Les *colored coins* rajoutent une couche logicielle au réseau bitcoin de façon à identifier un certain nombre de bitcoins, il devient donc possible de créer des marchés financiers, avec des actions ou des obligations, mais avec des coûts de fonctionnement nettement moins élevés que sur les Bourses existantes, car une organisation en réseau décentralisé s'avère moins coûteuse qu'une organisation centralisée nécessitant une ferme de serveurs.

Le *smart contract*

On peut aussi rédiger ce que l'on appelle des *smart contracts* (« contrats intelligents ») c'est-à-dire des opérations qui s'exécutent automatiquement ou sous condition. On peut programmer le fait que tel compte bitcoin versera telle somme à tel compte à une date précise. Ou que ce versement sera conditionné par un événement. Cela peut concerner le paiement d'une prestation une fois le travail effectué, par exemple. La blockchain, par sa sécurité et son immuabilité, assure que le contrat ne peut pas être modifié en cours de route par l'un des cocontractants, et par sa transparence, elle permet de vérifier la bonne exécution du contrat.

De façon plus élaborée, on peut construire un service d'assurance : les clients versent des cotisations sur un compte précis qui, en cas de dommage (vol, incendie, etc.) verse la somme prévue. Le dommage sera attesté par un tiers de confiance (un expert) choisi lors de la rédaction du contrat. Les coûts de fonctionnement seraient, là aussi, nettement inférieurs aux structures actuelles. Les *smart contracts* « permettent aux assurés comme aux assureurs de s'émanciper des phases déclaratives : formulaires, réclamation, vérification, déclenchement de l'indemnisation… La blockchain, en faisant office de tiers de confiance automatisé, ouvre la voie à une diminution des coûts de structure tout en fiabilisant et en accélérant les processus de décision[1] ».

1. « Blockchain et assurances », blockchainfrance.net.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

La *smart property*

Un autre type de service possible est l'authentification de documents, de droits de propriété (*smart property*). Il est possible d'enregistrer dans la blockchain une transaction précise qui intègre non pas le document lui-même, mais son empreinte (*via* un traitement cryptographique) et celle-ci devient une preuve horodatée, irréfutable et indélébile de l'existence de ce document sans avoir à en révéler le contenu, le tout pour un coût minime. C'est le métier des notaires et des organismes de dépôt de brevet qui est directement impacté.

L'enregistrement des droits de propriété constitue un des développements majeurs de la blockchain, c'est le cas du cadastre dans les pays émergents qui se révèle souvent déficient. Au Ghana, 90 % des terres rurales ne sont pas enregistrées dans une base de données officielle, ce qui constitue un réel frein au développement économique (conflits de voisinage, corruption, impossibilité d'hypothéquer le terrain pour emprunter, tout cela dissuade d'investir en infrastructures et contraint à se limiter à de l'autosubsistance). En accord avec l'État central, l'ONG Bitland s'attelle à enregistrer les titres de propriété sur la blockchain. Là encore, la mise en place d'un cadastre traditionnel, avec notaires et base de données centralisée, coûterait infiniment plus cher.

L'Organisation mondiale de la santé estime ainsi à 700 000 le nombre de décès par an provoqués par des médicaments contrefaits (10 à 30 % des médicaments fournis dans les pays en développement seraient des « faux médicaments »). Un moyen de lutter contre ce phénomène serait de créer un système universel garantissant la traçabilité des médicaments. « La blockchain, en tant que registre distribué, pourrait permettre aux différentes entreprises pharmaceutiques, aux régulateurs et même aux particuliers d'utiliser la même

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

base de données, sans qu'une seule entreprise ou institution n'en soit propriétaire[1]. »

Dans le domaine du commerce international, la technologie blockchain s'avère utile pour suivre les containers d'un bout à l'autre du monde : ils franchissent plusieurs frontières à travers plusieurs transporteurs, font l'objet de plusieurs paiements, ce qui génère quantité d'allers et retours d'informations, et des dépenses significatives (le traitement et l'administration de ces informations représentent près d'un cinquième des coûts du fret maritime). Les douanes, les ports, les transporteurs, les financeurs, etc., chacun possède sa propre base de données, son système informatique, ce qui nécessite d'incessants échanges, un back-office complexe et coûteux. Une blockchain partagée par ces acteurs et regroupant l'ensemble des caractéristiques des containers générerait d'importantes économies et des gains de temps.

Ubériser Uber !

Avec la blockchain il devient possible d'ubériser Uber ! Comment ? Les plates-formes Uber, Airbnb, Booking, BlaBlaCar, etc. ont pour point commun de centraliser les informations et les interactions entre les utilisateurs sur leurs serveurs, en prenant au passage une confortable commission (jusqu'à 25 % pour Uber ou Booking). Des applications décentralisées peuvent offrir le même service pour un coût nettement inférieur. Plus généralement, la blockchain remet en cause la façon même de s'organiser, que l'on conçoit toujours mentalement comme un processus de récupération de données, de centralisation, de mise en correspondance, puis de redistribution. La décentralisation casse le modèle hiérarchisé et lourd pour quelque chose de fluide et de transparent. La blockchain, c'est en quelque sorte « l'ubérisation ultime[2] ».

1. « La blockchain et la santé », blockchainfrance.net.

2. Expression de l'auteur, dans « Le blockchain, nouvel eldorado numérique des banques », *Le Monde*, 30 septembre 2015.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

Des blockchains… privées

Il se crée aussi des blockchains privées, même si cela peut sembler une contradiction sémantique pour ce processus fondé sur la transparence et la dimension publique. Les participants se choisissent entre eux et établissent une gouvernance ; nul ne peut entrer de son seul fait, il faut être agréé… Nous sommes loin de « l'esprit blockchain », on en revient à une structure centralisée. Les blockchains privées présentent des avantages qui peuvent expliquer l'intérêt que leur portent notamment les institutions financières : gouvernance simplifiée, acteurs connus, coûts réduits, rapidité, confidentialité. On pourrait les comparer aux Intranets, réservés à des utilisateurs précis, par opposition à l'Internet, public.

Les banques ont parfaitement compris l'intérêt de la blockchain pour transférer, stocker, échanger et gérer des actifs financiers de façon rapide, sécurisée et moins coûteuse que le système actuel, par exemple pour coter des actions ayant un faible volume de transactions, et donc mal adaptées au système centralisé actuel. Le consortium R3 réunit plus de 70 institutions bancaires actives dans ce domaine à travers le monde, mais les banques restent fidèles à leur « ADN », à leur culture du secret, et se concentrent sur les blockchains privées, où seul un nombre limité d'acteurs peut enregistrer des transactions ou disposer du registre.

Les DAO

Au-delà de ces différentes applications, il est possible d'élaborer une véritable « organisation décentralisée autonome » (DAO pour *Decentralized Autonomous Organisation*) définie par une multitude de *smart contracts* élaborés par une entreprise ou une communauté. Par exemple, OpenBazaar.org, un site de petites annonces semblable au Bon Coin, fonctionne à partir d'une DAO, si bien qu'aucune autorité centrale n'est nécessaire pour le faire tourner.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

Entièrement décentralisé, il ne génère aucun coût, il est donc gratuit pour l'utilisateur.

Une DAO apporte trois éléments nouveaux par rapport à une entité juridique traditionnelle[1] :

- une DAO ne peut pas être arrêtée ou fermée ;
- aucune personne ou organisation ne peut la contrôler (personne ne peut manipuler les chiffres ou modifier un contrat, par exemple) ;
- tout y est transparent et auditable, dans un cadre supranational.

Une DAO ne s'appuie pas sur le système juridique d'un pays considéré, elle est fondée sur du code informatique ce qui permet, normalement, d'éviter toute fraude[2].

« *Code is law* »

Derrière ces idées de *smart contracts* et de DAO, se trouve un principe formulé en 2000 par le juriste américain Lawrence Lessig : « *Code is law* », le code [informatique] est la loi. Les règles sont définies au départ et il est ensuite impossible d'en changer. Les parties prenantes peuvent ainsi effectuer des opérations précises en fonction d'instructions totalement auditables en garantissant une exécution non biaisée, puisque tous les contributeurs du réseau vérifient que personne n'a pu modifier le programme.

1. « Qu'est-ce qu'une DAO ? », blockchainfrance.net
2. Même si une DAO d'Ethereum (« TheDAO ») a été hackée, voir plus bas.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

Bitcoin, blockchain : un nouveau paradigme

Le bitcoin et la blockchain ne sont pas seulement de nouveaux « outils », c'est une nouvelle manière de voir les choses, une véritable révolution économique.

Un potentiel insoupçonnable

Tous les nouveaux services permis par la blockchain, encore embryonnaires aujourd'hui, qui permettent de sécuriser une somme d'argent, d'effectuer des paiements, de gérer des droits de propriété, de construire des marchés financiers et des systèmes d'assurance, constituent des outils fiables et bon marché capables de favoriser le développement économique. Les promoteurs de ces technologies « prédisent que la transition pourrait commencer par les pays instables, où la monnaie est faible, l'administration chaotique, la propriété privée mal protégée. Pour les nouvelles classes moyennes mondialisées de ces régions, la tentation sera forte de faire migrer leurs activités sur un réseau fiable, neutre, géré par des algorithmes incorruptibles[1] ».

Nous assistons à un vrai changement de paradigme pour le scientifique et prospectiviste Joël de Rosnay : « Pour la première fois dans l'histoire des révolutions technologiques, l'une d'entre elles, au-delà

1. « Dark Wallet, les anarchistes de l'argent », *Le Monde*, 18 octobre 2014.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

de la révolution Internet, a la capacité d'agir sur le pouvoir vertical et centralisé exercé par les États sur la monnaie, sur celui des banques et les transactions financières, des notaires et les cessions immobilières, des monopoles énergétiques sur la distribution d'électricité ou de carburants. Il semblait impossible d'imaginer de tels bouleversements avant le développement de la blockchain[1]. »

Les perspectives de tous ces services, dont beaucoup restent à inventer, sont potentiellement gigantesques. Des experts disent que le bitcoin, aujourd'hui, c'est Internet en 1995, c'est-à-dire le tout début du réseau quand seulement quelques applications avaient émergé (l'e-mail, les forums, les portails). Google attendra trois ans pour se lancer (décembre 1998), Facebook neuf ans (février 2004) alors que, techniquement, tout était en place dès le début, mais voilà, il fallait que quelqu'un en ait l'idée. Il en ira de même avec la blockchain.

La monnaie complémentaire pour tous

Le bitcoin n'est pas un phénomène isolé, il s'inscrit dans le vaste mouvement des monnaies complémentaires, c'est-à-dire de la volonté de sortir de la *monoculture monétaire*. Nous avons fini par l'oublier tant cela nous semble naturel et évident, mais l'euro, et le franc avant lui, sont des monnaies étatiques, officielles, obligatoires. C'est la seule monnaie dont nous disposons et nous n'imaginons pas en utiliser d'autre. Nos achats, notre épargne, nos impôts sont libellés en euros, et cela semble tout à fait naturel.

Une monnaie complémentaire est une monnaie qui peut être utilisée en complément de la monnaie officielle. Nul n'a obligation de faire ou de recevoir un paiement en monnaie complémentaire, cela se fait uniquement si le vendeur et l'acheteur sont d'accord. La monnaie étatique garde donc toute sa prééminence, mais elle n'est plus la seule.

1. « La blockchain décryptée », blockchainfrance.net, mai 2016.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

Les monnaies complémentaires constituent (en partie) une réponse aux risques bancaires (faillite) et monétaires (inflation). C'est à la suite de crises majeures qu'apparaissent les monnaies complémentaires. Elles se manifestent ainsi comme une réponse concrète, « qui vient d'en bas », face aux errements des dirigeants gouvernementaux et de la haute finance. Ces nouvelles monnaies permettent la réalisation d'échanges qui ne se seraient pas produits avec la monnaie étatique, elles introduisent de la « résilience » dans notre système financier[1].

Même si l'on compte aujourd'hui plus de 5 000 monnaies complémentaires dans le monde, en définitive, le nombre de personnes qui les utilise demeure restreint. Le phénomène, lui, est de plus en plus connu, mais ceux qui seraient disposés à l'essayer se rendent vite compte qu'ils n'en ont pas à portée de main. Quant à en créer une, cela relève tout de même d'un mécanisme complexe. Et quant aux personnes qui utilisent effectivement une monnaie complémentaire, elles constatent qu'elle n'est utilisable que localement et qu'il n'est pas possible de commercer avec une personne d'une autre ville, même si celle-ci possède également sa monnaie locale, car les deux monnaies ne sont pas convertibles. Très peu de monnaies complémentaires circulent dans l'ensemble d'un pays. Autre inconvénient, très peu d'entre elles sont acceptées sur Internet.

Le développement de monnaies complémentaires sur le modèle actuel ne peut pas suffire à répondre à la demande, ni à permettre à chacun d'avoir une alternative à sa monnaie officielle. C'est ici qu'intervient le bitcoin, né en janvier 2009. Voilà en effet une monnaie électronique et universelle : il suffit d'avoir une connexion Internet pour y avoir accès, et elle est valable dans le monde entier. Et si l'on n'est pas satisfait par cette monnaie, qu'à cela ne tienne, il en existe des dizaines d'autres, qui offrent des caractéristiques spécifiques.

1. Pour plus d'information voir Philippe Herlin, *La Fin des banques ?*, Eyrolles, 2015.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

Du cash sur Internet

L'idée semble contre-intuitive, pourtant elle est vraie : le bitcoin, c'est du cash sur Internet. Par « cash », on pense à des billets de banque que l'on tient en main, ce qui paraît antinomique du bitcoin. Mais quand on effectue une transaction avec de l'argent liquide, on ne rend de compte à personne, c'est un espace de liberté. Alors qu'un paiement électronique, par carte bancaire ou par virement, vous identifie et laisse des traces. Avec le bitcoin, on se retrouve dans le premier cas de figure : la transaction ne regarde que l'utilisateur, elle ne transite pas par le circuit bancaire. On est en fait sa propre banque !

Vu sous cet angle, le premier intérêt du bitcoin est d'apporter les services bancaires à tout le monde, et notamment à ceux qui en sont privés aujourd'hui, c'est-à-dire la moitié de la population mondiale. Dans les pays émergents, le taux de bancarisation est très faible et cela constitue un vrai frein au développement. Il n'est pas évident de lancer une quelconque activité en utilisant uniquement de l'argent liquide. Avec une connexion Internet, un simple smartphone connecté, et le taux d'équipement explose dans les pays émergents, tout le monde bénéficie d'un accès à des paiements en bitcoins, ou en n'importe quelle autre cryptomonnaie, ainsi qu'aux services permis par la blockchain. Les potentialités de développement s'ouvrent enfin à tous.

Autre intérêt : ceux qui craignent la disparition du cash (et les banques font tout pour cela), considérant que cela restreint leurs libertés, pourront basculer sur le bitcoin. La « guerre contre le cash » menée par les banques dans les pays développés risque de donner un sacré coup de fouet à l'utilisation du bitcoin !

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

Économie de la dette *versus* économie du cash

Un autre aspect fondamental doit être compris. Nous vivons dans une économie de la dette, tout est construit sur la dette : les dépenses des États, une partie significative de l'investissement des entreprises et des dépenses de consommation des ménages, l'essentiel du secteur de l'immobilier, de l'automobile, etc. Les politiques des banques centrales ne cherchent qu'à favoriser et à amplifier ce mouvement, avec leurs taux directeurs à zéro et leurs plans de rachat de dette souveraine (nommée « assouplissement quantitatif » ou, en anglais *quantitative easing*). Comme si la crise de 2008 n'avait pas servi d'avertissement, la dette mondiale (publique et privée) a encore augmenté depuis cette date, selon l'Institute of International Finance, pour atteindre désormais 324 % du PIB mondial[1]…

Le bitcoin, lui, c'est du « cash sur Internet », un système monétaire construit sur une ressource rare (les 21 millions de bitcoins), sans banque centrale qui joue sur les manettes de son tableau de bord, sans banque du tout d'ailleurs, puisqu'il circule sur Internet. Un fonctionnement qui évoque immédiatement l'étalon-or, l'époque où la quantité d'or reposant dans les banques centrales conditionnait la quantité de monnaie en circulation, et interdisait toute explosion de la dette publique, et son financement par les banques centrales.

Le bitcoin n'a pas pour objectif de remplacer le système monétaire actuel, il faudrait pour cela une décision concertée des grands États, ce qui serait très peu conforme à l'esprit « rebelle » qui a présidé à sa fondation, et cela signifierait également que ces États acceptent de se dessaisir de tout pourvoi monétaire, ce qui est inconcevable.

1. « La dette mondiale atteint 324 % du PIB de la planète, selon une étude », Reuters, 25 octobre 2017.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

Mais le bitcoin serait un îlot de monnaie saine, non manipulée, que chacun serait libre d'utiliser.

Aujourd'hui, le cours du bitcoin est trop volatil, mais avec le temps, lorsqu'il sera plus stable et qu'il concernera beaucoup plus de monde, chacun pourra comparer les deux systèmes, entre celui dopé aux liquidités, exposé à l'inflation et aux crises bancaires, et celui fondé sur une monnaie saine.

Une gouvernance originale

Issu d'une tradition anti-autoritaire, le bitcoin ne pouvait fonctionner autrement que par consensus. Le problème est qu'il faut accorder des acteurs ayant chacun des intérêts spécifiques : les développeurs, qui font évoluer Bitcoin Core, le logiciel open source qui fait tourner le bitcoin (« les gardiens du temple »), les mineurs, qui vérifient les transactions et achètent du matériel dédié et de l'électricité, les places de marché, qui font des transactions en bitcoins contre du dollar, du yen, du yuan ou de l'euro, les start-up, qui se lancent sur la blockchain, les grandes banques, les multinationales, les GAFA, qui se penchent de près sur cette technologie.

En cas de désaccord, étant donné que l'algorithme qui fait tourner le bitcoin est open source, chacun est libre de le copier, de modifier quelques paramètres et de créer une nouvelle monnaie. Mais parfois, il se produit quelque chose de tout à fait original pour une monnaie, mais absolument normal dans le domaine du logiciel libre : un fork, c'est-à-dire qu'une partie de la communauté part créer sa monnaie sur la base du bitcoin. Ce phénomène de « *fork* » (fourche en anglais) est courant dans le secteur du logiciel libre : beaucoup disparaissent mais certains réussissent comme la plate-forme de blogs Wordpress née du fork du logiciel de blog « b2 » qui, lui, est tombé dans l'oubli, l'éditeur de site Joomla né d'un fork de Miro, etc.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

Mais avec le bitcoin, il se passe une chose supplémentaire : compte tenu de l'existence de la blockchain, de l'historique des transactions, tous ceux qui détiennent des bitcoins à la date du fork reçoivent le même nombre d'unités de la nouvelle monnaie ! On l'a vu lors du fork du 1er août 2017, celui qui détenait par exemple 3 bitcoins a récupéré, automatiquement sans rien demander, 3 Bitcoins Cash, qui valaient sur le marché environ un dixième du prix du bitcoin. Sur le moment, on a l'impression de recevoir de l'argent qui tombe du ciel, mais cela pose aussi des problèmes, nous y reviendrons.

La question de la confiance

La blockchain renouvelle la question de la confiance. Suivons le raisonnement d'Alexandre Stachtchenko[1], cofondateur de Blockchain France, qu'il développe avec des talents d'évangélisateur. « Internet a échoué affirme-t-il, l'Occidental moyen s'est appauvri, les inégalités se creusent, les libertés individuelles sont menacées, le pouvoir n'a jamais été aussi centralisé. Internet a promis un monde où l'individu s'affirmait, reprenait le pouvoir, grâce à un réseau décentralisé, mais Internet a échoué, les GAFA centralisent tout le pouvoir. »

Il pose ensuite la question : « Qu'est-ce qui manque aujourd'hui ? Quelle est cette ressource cruciale qui manque, qui explique l'éclatement successif des bulles financières, la crise sociale, la crise identitaire, la crise européenne ? Est-ce que c'est l'argent ? Non, le monde n'a jamais été aussi riche. Est-ce que c'est le lien social ? Non, grâce à Internet, le monde n'a jamais été aussi connecté. Ce qui manque, c'est la *confiance*. Tout le temps, on en parle, de cette confiance : confiance dans les marchés, confiance dans les gouvernements, confiance dans

1. « Alexandre Stachtchenko, cofondateur de Blockchain France à la Cloud Week Paris le 4 juillet 2016 », YouTube.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

l'Union européenne, etc. À chaque fois qu'on parle de la confiance, c'est pour souligner son absence. »

Selon lui, « la question phare, c'est comment faire confiance, comment avoir confiance dans l'information, dans les gouvernements, dans les banques, qui gèrent mal de l'argent qu'elles n'ont pas pour faire toujours plus de profits ».

Il rappelle que Satoshi Nakamoto fait ce constat, pour les banques, et qu'il propose de s'en passer en créant une nouvelle monnaie électronique décentralisée, c'est le bitcoin. Mais le bitcoin n'est pas qu'une monnaie, c'est aussi la blockchain. Voici la définition qu'il en donne : « La blockchain est un protocole numérique gérant un réseau pair à pair qui enregistre la propriété et crée la confiance », et le détail qu'il fait de ce sur quoi elle repose :

- « [le] protocole numérique, c'est-à-dire un ensemble de règles pour que les machines se comprennent entre elles » ;
- un réseau « décentralisé : chaque pair est égal, sans hiérarchie » ;
- la propriété numérique : « Internet permet l'échange d'informations mais le problème est que sur Internet vous pouvez dupliquer l'information autant de fois que vous voulez. Si je vous envoie un morceau de musique, vous pouvez le copier dix fois, cent fois. Vous ne pouvez donc pas échanger de la valeur sur Internet, parce que la valeur vient de la rareté, donc si vous pouvez dupliquer n'importe quel bout de valeur, votre valeur disparaît. Et donc la blockchain vient permettre cet échange de valeur sur Internet en identifiant chaque bout d'information, en traçant chaque bout d'information, créant ainsi la propriété numérique, et la confiance. »

On revient ici au début de notre livre lorsque nous expliquions le fonctionnement du bitcoin : l'enjeu consistait à faire circuler un objet numérique infalsifiable sur Internet, où la duplication est pourtant consubstantielle au monde numérique. Le bitcoin y est parvenu, mais

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

la blockchain permet à n'importe quel objet numérique de bénéficier de cette découverte : un morceau de musique, un brevet, un droit de propriété, une transaction commerciale. Le vote électronique devient possible parce que transparent dans son organisation, alors que les outils actuels, centralisés, suscitent justement la méfiance.

Continuons avec Alexandre Stachtchenko : « La monnaie est une application de la blockchain, mais c'est loin d'être la seule. Pourquoi faut-il s'intéresser à la blockchain ? Parce qu'elle a le potentiel de toucher à la confiance, c'est-à-dire de changer la majorité de nos comportements en créant des possibilités inédites, et ce dans tous les sujets majeurs de ce début de siècle. Elle permet à 3,5 milliards d'individus non bancarisés d'accéder à des services financiers, elle permet de créer de la confiance dans des situations où elle n'existe pas, du fait d'États faillis, de lobbying, etc. » Il conclut, lyrique : « On se prend à rêver que la blockchain crée un monde plus humain, plus juste. »

Prolongeons la réflexion : il n'y a pas qu'Internet qui a échoué, il y a aussi les États qui, parfois, entraînent leur pays dans la guerre, la faillite ou la corruption, ou, dans nos démocraties libérales, qui cherchent à s'occuper de tout et déresponsabilisent ainsi les individus. Avec un outil comme la blockchain, il devient possible à des communautés de s'organiser de façon autonome, de se prendre en main, de façon transparente et peu coûteuse. Cela ne peut avoir que des effets positifs.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

pyright © 2018 Eyrolles.

Les contre-vérités sur le bitcoin

Répondons aux critiques les plus souvent formulées à l'encontre du bitcoin.

Non, le bitcoin n'est pas anonyme

L'anonymat du bitcoin est souvent décrié (« la monnaie de la drogue et des mafias »), mais il faut comprendre qu'il est tout à fait relatif. Bien sûr, les adresses sont confidentielles et chacun peut en créer autant qu'il veut, cependant les transactions sont publiques et restent à jamais indélébiles (dans la blockchain, la base de données des transactions), elles constituent une « preuve » absolue et incontestable des transferts d'argent. Une adresse qui reçoit et envoie des montants importants peut être facilement repérée et mise sous surveillance par n'importe quel organisme officiel de lutte contre le blanchiment, ainsi que l'ensemble de ses correspondants. Ce n'est pas précisément ce que recherchent les organisations criminelles.

D'autre part, si le réseau peut être relativement anonyme, le fait d'y entrer ou d'en sortir laisse des traces aisément identifiables. Un compte est facilement identifié à partir du moment où il quitte le réseau bitcoin : soit il vend ses bitcoins sur une place de marché et vire les euros obtenus en contrepartie sur un compte en banque,

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

ce qui le relie à coup sûr à une personne physique, soit il achète un produit chez un marchand, et révèle ainsi un domicile. Dans l'autre sens, pour acheter des bitcoins, il faut obligatoirement passer par un compte bancaire, on ne peut pas en acquérir avec des valises de billets, on est donc également identifié. Il faut ainsi plutôt parler de pseudo-anonymat (« pseudonymat »). Un site américain s'était fait une réputation de vendre de la drogue en échange de bitcoins, il se nommait Silk Road. Lorsque le FBI l'a fermé le 3 octobre 2013, on n'a noté aucune baisse du cours, preuve que les trafics illicites comptent pour quantité négligeable dans le bitcoin.

L'argent de la drogue et des trafics illicites utilise depuis longtemps le cash et le circuit bancaire offshore, de grandes banques ayant pignon sur rue sont régulièrement impliquées. Le bitcoin est trop visible et trop lisible pour offrir une alternative intéressante.

Si, le bitcoin a une valeur intrinsèque

Ce n'est que du code informatique, du « vent », disent ses détracteurs. Cette remarque est déjà stupide en soi, Facebook aussi ce n'est que du « code », cela ne vaut-il donc rien pour autant ? Cela peut-il disparaître soudainement ? Affirmer cela traduit surtout une méconnaissance totale de l'informatique et d'Internet. Le Prix Nobel Jean Tirole tombe dans ce piège : « C'est quelque chose qui n'a pas de valeur intrinsèque, qui peut s'effondrer du jour au lendemain. Donc, je ne voudrais absolument pas que les banques françaises, par exemple, investissent dans le bitcoin[1]. »

Alors, d'où vient la valeur du bitcoin ? Qu'est-ce qui fait intrinsèquement sa valeur ? Voici une question qui suscite encore aujourd'hui des discussions et des polémiques. Essayons d'y voir clair.

1. « Le bitcoin, une "monnaie ubérisée" mais pas sans danger », lepoint.fr *via* AFP, 24 novembre 2017.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

Une monnaie-papier comme l'euro n'a pas de valeur intrinsèque, c'est un morceau de papier, ou une écriture électronique dans le système bancaire. C'est surtout la contrepartie d'une dette. Un billet de 10 euros constitue, pour celui qui le détient, un actif. Mais ce billet est aussi inscrit au passif de la Banque centrale européenne (BCE), et si celle-ci use et abuse de la planche à billets, elle diminue le pouvoir d'achat de la monnaie, sans qu'on n'y puisse rien. C'est comme une action, qui figure au passif de l'entreprise (son capital), et qui perd de la valeur si l'entreprise fait des pertes, ou même ne vaut plus rien si elle fait faillite.

Au contraire, l'or est sans contrepartie, il ne figure au passif de personne, il possède une valeur intrinsèque (c'est aussi le cas pour un bien immobilier, une œuvre d'art). « L'or ne fait pas faillite », affirme le dicton, effectivement, et c'est ce qui fait toute sa valeur, notamment en période de crise financière. Bien sûr, son cours exprimé en euros varie avec le temps, mais il garde une valeur intrinsèque par-delà les décennies.

Le bitcoin, comme l'or, est sans contrepartie, il ne dépend d'aucune institution, il n'est inscrit au passif de personne, et c'est ce qui fait toute sa force. Mais quelle est sa valeur intrinsèque justement ? Il n'y a pas de réponse définitive à cette question. Sur le site du projet, bitcoin.org, on peut lire : « Bitcoin tire sa valeur de son acceptation comme moyen de paiement. Sa valeur initiale sur le marché a été obtenue lorsque les gens ont spéculé et que, de par ses propriétés, la monnaie allait être acceptée ensuite par d'autres. » C'est certain, mais pas suffisant car un peu tautologique (le bitcoin a de la valeur parce qu'il est accepté comme moyen de paiement) et trop fondé uniquement sur la confiance, comme les monnaies-papier.

L'économiste Georges Lane, adepte de l'école autrichienne, apporte un élément déterminant à cette question en expliquant que : « Le système de paiement est la source de la valeur, tandis que l'unité

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

de compte se borne à exprimer cette valeur en termes de prix[1]. » Effectivement, l'euro n'est pas en lui-même un système de paiement (hormis le cas où je paye de la main à la main en liquide), les transactions passent par des intermédiaires (banque, carte de paiement, Paypal, etc.). *Idem* pour l'or d'ailleurs où, à part le paiement de la main à la main, il faut s'en remettre à un intermédiaire ou transporter cet or, ce qui représente un coût et un risque. Au contraire le bitcoin est d'abord un système de paiement (avant d'être une unité monétaire), et celui-ci fonctionne parfaitement et pour un coût minime, et c'est ce qui fait toute sa valeur.

Il faut bien comprendre cette distinction : l'euro n'est pas un système de paiement, quand on paye par carte bancaire, on passe par une banque. L'euro est « seulement » une monnaie, pour circuler il doit passer par le système bancaire. Alors que le Bitcoin est d'abord un système de paiement, efficace, rapide, peu coûteux, et qui transite par Internet, c'est-à-dire complètement en dehors du circuit bancaire (le Bitcoin – avec un B majuscule – est le système de paiement, la blockchain, le bitcoin – avec un b minuscule – est la monnaie qui circule). La « qualité » de ce système de paiement fait sa valeur.

Ajoutons que cette unité monétaire, le bitcoin, est disponible en quantité limitée (pas plus de 21 millions), ce qui en fait une ressource rare, donc coûteuse.

Ajoutons également à cette analyse que le paiement n'est pas la seule option permise par le bitcoin, mais que la blockchain permet aussi d'implémenter quantité d'applications et de services financiers qui concourent pareillement à cette valeur intrinsèque. C'est le protocole, ou l'algorithme, qui confère au bitcoin sa valeur intrinsèque.

Alors, que vaut un bitcoin ? Justement, personne n'a le pouvoir d'en décider puisqu'il n'y a pas de banque centrale ou d'autorité légale. Le bitcoin est une monnaie complémentaire, alternative, ce qui signifie

1. « Ce qui a donné au "bitcoin" toute sa valeur », 24hGold, 13 juillet 2017.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

que le vendeur et l'acheteur doivent être d'accord pour réaliser une transaction dans cette monnaie – personne n'est obligé de recevoir un paiement en bitcoin contre sa volonté (contrairement à l'euro qui a « cours légal » dans toute la zone euro). La réponse est donc simple : ce sont ceux qui l'utilisent qui vont en fixer le prix. C'est l'offre et la demande qui déterminent le cours du bitcoin contre les principales devises.

Non, le bitcoin n'est pas une pyramide de Ponzi

« La hausse alimente la hausse, jusqu'à l'écroulement final », affirment ceux qui assimilent le bitcoin à un schéma de Ponzi. Un système de Ponzi est un produit financier qui promet un taux d'intérêt exceptionnellement élevé, et qui le verse effectivement aux premiers souscripteurs… avec l'argent déposé par les clients. Tant que les nouveaux arrivants affluent, le système s'entretient et son initiateur s'en met plein les poches, jusqu'à ce que les retraits dépassent l'argent en caisse, alors la pyramide s'écroule.

Mais dans un système de Ponzi il n'y a aucune création de valeur. Les taux d'intérêt versés proviennent du capital déposé, pas d'une quelconque activité économique. Au contraire, le bitcoin génère de la valeur à plusieurs niveaux : comme moyen de paiement, comme ressource rare, avec la blockchain comme support de multiples applications ; tout un écosystème se développe autour de lui. De plus, avec Bitcoin et la blockchain, nous avons affaire à un nouveau paradigme (un fonctionnement en réseau décentralisé) qui va impacter d'une façon ou d'une autre la plupart des secteurs de l'économie, il est donc normal que l'on assiste à l'arrivée de tant de nouveaux investisseurs, d'utilisateurs, et de start-up.

Et puis, il ne faut pas analyser les choses à l'envers : ce n'est pas parce que quelque chose a du succès et voit son nombre d'adeptes

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

exploser qu'il s'agit d'un système de Ponzi ! Sinon Apple est un système de Ponzi, Facebook aussi, ainsi que le smartphone, Internet, etc.

Non, le bitcoin n'est pas une bulle

Dans la même veine que l'accusation précédente, le bitcoin serait une bulle : le cours monte uniquement grâce aux nouveaux arrivants. Non, le bitcoin possède une valeur intrinsèque, tout un écosystème se développe, nous l'avons vu.

Maintenant, il ne faut pas exclure qu'il y ait une dimension bullaire dans la hausse du cours, évidemment. Une bulle apparaît lorsque le prix du marché s'écarte de façon excessive de la valeur intrinsèque, et la forte volatilité du bitcoin semble indiquer que cela se produit de temps à autre. À de fortes hausses succèdent souvent des mini-krachs, les périodes de « montagnes russes » sont courantes.

Mais fondamentalement, le bitcoin n'est pas une bulle parce que son succès ne se résume pas au nombre de ses acquéreurs, on compte aussi de plus en plus d'utilisateurs (pour des transactions), de nouvelles applications de la blockchain.

Et si la « bulle du bitcoin » avait en fait déjà éclaté ?

On nous parle sans cesse d'une « bulle du bitcoin » qui menacerait d'éclater à tout moment : et si, en fait, cet événement avait déjà eu lieu ? C'est l'analyse originale et pertinente qu'expose le site AllStart[1]. Le bitcoin a déjà connu un effondrement puisque entre le plus haut niveau atteint en novembre 2013 et le plus bas niveau atteint fin 2014,

1. « Pourquoi la bulle de Bitcoin a déjà éclaté ? », journalducoin.com, 4 novembre 2017.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

le cours a perdu 86 %. Si ce n'est pas une bulle qui explose, qu'est-ce d'autre ?

Et ce profil d'un krach suivi d'une montée progressive et irrésistible se retrouve dans le cas de grandes entreprises cotées comme Amazon (95 % de chute en 2000) ou Nvidia (85 % de chute en 2000) ; la ressemblance des graphiques est frappante, pour l'effondrement comme pour la progression qui suit. Bien sûr, de nombreuses sociétés ont disparu lors du krach de la bulle Internet en 2000, mais celles qui ont survécu sont devenues très fortes.

Évidemment, cela ne veut pas dire qu'il n'y aura pas à l'avenir de sévères corrections, pour le bitcoin comme pour Amazon, mais la forte croissance du cours du bitcoin s'est déjà vue. L'auteur de l'article conclut : « C'est un fait, une bulle du bitcoin a déjà éclaté récemment, il s'est redressé, et maintenant, il se comporte comme les actifs à tendance haussière se sont toujours comportés. Rien d'inhabituel. »

Non, le bitcoin ne va pas remplacer les autres monnaies

Il n'y a pas de « complot ». Le bitcoin ne va pas éradiquer les monnaies existantes. Contrairement aux grandes devises, il n'y a pas d'État ou de multinationale derrière le bitcoin, aucune loi ne l'impose nulle part, personne n'est obligé de l'utiliser. Vous ne croyez pas dans le bitcoin ? Fort bien, ne l'utilisez pas, personne ne vous y contraindra. Alors que si vous doutez de l'euro, vous ne pouvez pas faire sans : vos salaires et rémunérations sont versés en euros, vous devez payer vos impôts en euros, les contrats que vous signez sont rédigés dans cette monnaie, etc.

Le bitcoin et la blockchain se feront leur place dans la mesure où ils convaincront de leur utilité, et uniquement pour cette raison, et ils cohabiteront avec les autres monnaies. Mais c'est aussi à ces dernières

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

de montrer leur solidité et à leurs systèmes bancaires de démontrer leur efficacité, car désormais, il y a de la concurrence.

Non, le bitcoin n'a pas besoin d'une banque centrale

Selon certains[1], le bitcoin échouera du fait de l'absence d'une banque centrale, notamment à travers l'une de ses principales missions, celle de « prêteur en dernier ressort ». En cas de crise financière de type 2008, aucune banque centrale ne pourrait intervenir pour sauver les banques qui auraient fait des prêts en bitcoins, ce qui entraînerait une vague de faillites catastrophique.

Cette critique est particulièrement révélatrice, car c'est précisément parce qu'il existe des banques centrales interventionnistes que nous connaissons de graves crises financières : si les banques commerciales sont assurées d'être secourues, elles vont prendre d'autant plus de risques ! C'est le syndrome, désormais largement étudié et reconnu, du *too big to fail* (trop gros pour faire faillite), qui pousse les autorités monétaires et gouvernementales à venir au secours des banques menacées d'effondrement. Ne pouvant bénéficier d'un tel secours, une banque qui voudrait faire des prêts libellés en bitcoins prendrait des garanties autrement plus solides que les banques actuelles.

L'absence de banque centrale empêche la planche à billets, autrement nommée « assouplissement quantitatif » pour noyer le poisson, c'est-à-dire de remettre en cause la limite de 21 millions de bitcoins et d'en créer un ou deux millions de plus. Non vraiment, l'absence de banque centrale est à considérer comme un point fort du bitcoin !

1. « BNP Paribas : le Bitcoin va échouer du fait de l'absence d'un "prêteur en dernier ressort" », crypto-France.com, 20 novembre 2017.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

Une histoire mouvementée

Suivons l'évolution du cours du bitcoin et des événements importants qui l'ont impacté.

2009, le lancement

Son lancement a lieu le 3 janvier 2009, on le rappelle et il circule entre quelques geeks, dont le fameux Satoshi Nakamoto. Au début, c'est simple, le bitcoin ne vaut rien. Le 5 octobre 2009 est publié le premier taux de change bitcoin/dollar, il vaut environ 0,001 dollar américain, un dixième de centime…

2010, la première transaction

Le 22 mai 2010 a lieu la première transaction dans le monde réel : sur un forum, un développeur propose 10 000 bitcoins pour deux pizzas, le bitcoin vaut alors 0,003 dollar (soit 30 dollars pour les deux pizzas). Cet événement fondateur est devenu la « fête du bitcoin » et tous les ans, le 22 mai, est célébré le « Bitcoin Pizza Day » où les utilisateurs de bitcoins sont invités eux aussi à s'offrir des pizzas. C'est à cette époque que commencent à apparaître les premiers marchands acceptant les bitcoins. Ces 10 000 bitcoins valent aujourd'hui une véritable fortune – on espère que les pizzas étaient bonnes.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

Le 12 décembre 2010 est posté le dernier message de Satoshi Nakamoto sur le principal forum. Il quitte le projet, annonçant simplement être passé à autre chose. Il passe la main à Gavin Andresen en lui confiant la clé d'alerte (qui permet de publier une alerte à tous les « clients » bitcoin, c'est-à-dire les nœuds du réseau).

2011, début d'intérêt des médias

En février 2011, un bitcoin vaut 1 dollar.

Survient, en juin 2011, une première bulle (30 dollars), quand quelques journaux américains sortent des articles, mais elle est immédiatement suivie d'un krach lorsqu'une importante place de marché (Mt. Gox) se fait hacker. Le cours tombe à son plus bas taux en décembre 2011, sous les 3 dollars, et les rares articles publiés à l'époque considèrent pour la plupart que la monnaie n'a aucun avenir et va disparaître.

2012, naissance de l'intérêt pour la blockchain

En octobre 2012, la Banque centrale européenne publie un premier rapport sur les monnaies virtuelles, dont le bitcoin.

Le 28 novembre 2012, la récompense de minage est divisée par deux (comme ce sera le cas tous les 4 ans) et passe de 50 à 25 bitcoins (on parle de « *halving* »).

Le 4 décembre 2012, le mathématicien israélien Meni Rosenfeld publie un article de recherche sur les *colored coins*, un métaprotocole qui permet d'associer des actifs réels à des adresses Bitcoin. C'est le début de la blockchain comme champ d'expérimentation.

Tout au long de l'année, le cours monte progressivement pour passer en décembre la barre des 10 euros.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

2013, l'année du bitcoin

2013 est « l'année du bitcoin » : il sort de l'anonymat, les grands médias de la planète se mettent à en parler.

Le cours du bitcoin connaît une première progression importante avec un sommet à 287 euros le 9 avril 2013. C'est la crise chypriote qui provoque cet engouement : pour la première fois dans un pays moderne, les banques, afin de se renflouer, ponctionnent les comptes de leurs clients ! Le choc est énorme et des défenseurs du bitcoin, repris par les médias, font remarquer que le bitcoin est à l'abri d'une telle mésaventure puisqu'il ne circule pas dans le système bancaire. Mais le cours s'effondre dès le lendemain, le 10 avril, pour fluctuer autour de 80 à 100 euros jusqu'à la fin de l'été.

Le 2 octobre 2013, le site clandestin Silk Road est fermé par le FBI. Cette plate-forme vendait toutes sortes de produits illicites utilisant le bitcoin comme paiement. Cette nouvelle rassure les investisseurs et le cours du bitcoin entame une nouvelle progression. Il faut dire qu'à cette époque, le bitcoin est très souvent associé par la presse à des transactions frauduleuses (drogue, argent sale). Le fait que la fermeture de Silk Road ne provoque pas d'effondrement du cours démontre que ces trafics illicites étaient marginaux.

Puis le cours repart dans une fulgurante hausse lors du mois de novembre 2013 (le chiffre symbolique des 1 000 dollars [800 euros] est franchi le 28 novembre) : les Chinois découvrent le bitcoin et une bulle se crée. La Chine devient, et elle le demeure encore aujourd'hui, le principal pays pour le minage du bitcoin. Elle bénéficie en effet d'une électricité hydroélectrique peu coûteuse et d'une puissante industrie de composants informatiques qui fabrique les ASIC (*Application-Specific Integrated Circuit*) permettant de miner. L'attrait pour la spéculation et le goût pour la technologie font le reste.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

En décembre 2013, la Banque populaire de Chine met le holà, et commence par interdire le bitcoin, avant de l'autoriser à nouveau quelques semaines plus tard, mais le cours décroche à 600 euros.

2014, acceptation par les autorités

La fermeture du site Mt. Gox, la principale plate-forme d'échange de bitcoins, en février 2014, crée désillusions et doutes par rapport au bitcoin. La plate-forme était mal gérée, le bitcoin en lui-même n'est en rien responsable, mais en termes d'image, le résultat s'avère très négatif. Le cours baisse régulièrement durant 2014 pour se stabiliser un peu au-dessus de 200 euros.

Le 13 mai 2014 est inaugurée La Maison du bitcoin à Paris[1] premier établissement « en dur » consacré à la cryptomonnaie.

Les années 2013 et 2014 marquent une généralisation dans le monde de l'intérêt des instances politiques, des banques centrales et des régulateurs pour le bitcoin, dans un sens globalement favorable.

2015, l'année de la blockchain

2015 est « l'année de la blockchain ». En octobre, l'hebdomadaire *The Economist* fait sa une sur la blockchain (« The Trust Machine ») annonçant que « la technologie derrière le Bitcoin pourrait changer le monde ». La réputation du magazine, très lu dans les milieux économiques, permet alors à la blockchain de sortir des cercles geeks et lui donne une crédibilité quasi institutionnelle. Durant cette année, plusieurs grandes sociétés annoncent leur intérêt pour cette technologie (UBS, Orange, IBM, etc.).

Le cours végète quant à lui dans la zone des 200 euros.

1. 35, rue du Caire, 75002 Paris.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

2016, une progressive montée en puissance

La hausse du cours s'amorce durant le dernier trimestre 2015, et l'année 2016 marque une progression régulière, jusqu'à dépasser le chiffre symbolique de 1 000 dollars (950 euros) le 1er janvier 2017.

Le 9 juillet 2016 a lieu la deuxième division par deux de la récompense des mineurs qui passe de 25 à 12,5 bitcoins. Le premier *halving* avait eu lieu le 28 novembre 2012. Le cours est alors à 590 euros.

Le réseau bitcoin commence à saturer, les développeurs et les mineurs réfléchissent à des mises à jour afin de résoudre ce problème.

2017, l'explosion du cours

Le bitcoin dépasse la valeur symbolique des 1 000 euros le 4 janvier 2017. La Banque populaire de Chine intervient une nouvelle fois brutalement (elle était déjà intervenue en décembre 2013) le 11 janvier 2017 avec un « rappel à l'ordre » aux plates-formes chinoise de trading ; elle ne veut pas que le bitcoin permette de contourner de façon massive le contrôle des changes, ce qui fait chuter le cours sous les 800 euros, qui repartira toutefois rapidement à la hausse. Autant la hausse de novembre 2013 était fulgurante et ne pouvait déboucher que sur une sévère correction, autant la hausse progressive du cours sur toute l'année 2016 indique que des forces pérennes sont à l'œuvre (nous verrons lesquelles ensuite).

Un quadruplement du cours se produit d'avril à début septembre, le bitcoin passant de 1 000 à plus de 4 000 euros ! On peut interpréter cette formidable progression comme l'implémentation réussie de Segwit, une amélioration du protocole afin d'augmenter le nombre de transactions. L'opération se déroule bien, la confiance dans le réseau bitcoin se renforce et s'étend. Concomitamment, l'explosion du cours attire de nouveaux adeptes, de nouveaux acheteurs : le 2 novembre

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

2017, la principale place de marché américaine, Coinbase, annonce 100 000 nouveaux clients en 24 heures…

Mais l'implémentation de Segwit déplaît à un certain nombre de bitcoiners, très minoritaires, qui déclenchent un hard fork et créent donc une nouvelle cryptomonnaie, le Bitcoin Cash (BCH). Son cours tombe rapidement à un dixième de bitcoin et ne semble guère performer depuis. Tous ceux qui possédaient des bitcoins ce 1er août 2017 récupèrent le même nombre de Bitcoins Cash, comme de l'argent qui tombe du ciel… Mais on peut considérer que si ce fork n'avait pas eu lieu, le bitcoin aurait davantage progressé, de l'équivalent de la valeur du Bitcoin Cash.

Une autre modification importante était prévue pour le 16 novembre 2017. Dénommée Segwit2x, elle était soutenue par 80 % des mineurs, mais refusée par la grande majorité des développeurs. Jamais un conflit aussi tranché ne s'était produit dans la communauté bitcoin. On allait tout droit vers un nouveau hard fork, qui comportait en outre des menaces techniques significatives, lorsqu'à la surprise générale, le 8 novembre, ses promoteurs décident d'abandonner cette mise à jour en expliquant dans un communiqué que : « Notre objectif a toujours été d'améliorer Bitcoin en douceur. Bien que nous croyions fermement à la nécessité de l'augmentation de la taille des blocs, il y a quelque chose que nous croyons encore plus important : garder la communauté unie. Malheureusement, il est clair que nous n'avons pas encore atteint un consensus suffisant pour une mise à niveau propre. Poursuivre dans la voie actuelle pourrait diviser la communauté et constituer un problème pour la croissance de Bitcoin. Ce n'a jamais été le but de Segwit2x. […] Bitcoin reste la meilleure forme de monnaie jamais vue par l'humanité, et nous restons déterminés à protéger et à favoriser sa croissance dans le monde entier. » C'est une excellente nouvelle qui montre la maturité et l'intelligence de la communauté Bitcoin au sens large (utilisateurs, places de marché, développeurs, mineurs). Nous pouvons continuer d'être très optimistes pour l'avenir du bitcoin.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

Le 11 décembre sont lancés les premiers contrats à terme sur le bitcoin sur le CME (*Chicago Mercantile Exchange*), d'autres marchés boursiers ont annoncé des initiatives comparables. Ces annonces provoquent une forte hausse du cours du bitcoin durant les deux premières semaines du mois de décembre, où il dépasse les 16 000 euros, mais il corrige ensuite sérieusement en passant sous la barre des 11 000 euros, soit un krach de plus de 30 %, finalement assez habituel dans la vie tumultueuse qui est la sienne. Au final, sur l'année 2017, le bitcoin a vu son cours multiplié par 11, une performance exceptionnelle. 2017 restera aussi comme « l'année des ICO », nous allons y revenir en détail plus loin.

2018, l'arrivée des investisseurs institutionnels

La création de contrats à terme et d'ETF marquent l'arrivée des investisseurs institutionnels dans les cryptomonnaies. De nombreux fonds ont été créés dans le second semestre 2017, voilà qui devrait soutenir la progression du cours dans l'année 2018, avec la continuation de l'arrivée des investisseurs particuliers.

À la mi-janvier, le cours du bitcoin connaît une sévère correction en tombant sous les 8 000 euros, soit une division par deux de son record atteint un mois plus tôt ! La volonté des autorités chinoises et coréennes d'interdire les achats anonymes sur les plateformes d'échange explique en grande partie ce mouvement de panique. Cette volatilité extrême s'avère en réalité assez courante pour le bitcoin et les cryptomonnaies en général, il ne faut pas craindre les montagnes russes !

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

pyright © 2018 Eyrolles.

Les principales autres cryptomonnaies

Pendant plusieurs années, le bitcoin fut seul ou presque, puis largement dominant quand bien même de nombreuses cryptomonnaies faisaient leur apparition. Ce n'est désormais plus le cas, même s'il reste numéro un, il doit cohabiter avec d'autres.

Comment naissent les cryptomonnaies ?

Pourquoi d'autres cryptomonnaies apparaissent-elles ? Parce que le bitcoin à lui tout seul ne peut pas satisfaire tous les utilisateurs potentiels, ni tous les besoins, parce que des entrepreneurs tentent de proposer une cryptomonnaie plus efficace sur tel ou tel point, ou identifient des faiblesses et veulent y répondre. Le secteur des cryptomonnaies est ultraconcurrentiel et non régulé, à peu près n'importe qui peut créer sa « crypto ».

Justement, comment se créent les cryptomonnaies ? On peut identifier trois méthodes.

La copie du code bitcoin

La base de données des transactions du bitcoin (la blockchain) est publique, nous l'avons dit, mais le programme lui-même bien sûr, contrairement à Windows par exemple pour lequel un « noyau »

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

demeure inaccessible, pour protéger le cœur du programme ainsi que les droits de propriété intellectuels de Microsoft. Personne n'aurait confiance dans le bitcoin si plusieurs lignes de programmes restaient à jamais cachées. La contrepartie, ou la conséquence si l'on préfère, de cette transparence est que n'importe qui peut copier ce programme, le modifier à la marge et créer ainsi sa propre monnaie numérique. Il en existe plus de 1 000[1] et, il faut le dire, un grand nombre d'entre elles sont soit farfelues (UFO Coin, Ovni en anglais), soit anecdotiques de par le faible volume qu'elles représentent.

Des forks du bitcoin

Créer une cryptomonnaie à partir de rien se révèle très difficile, il faut inciter des mineurs à faire « tourner la machine », recruter des utilisateurs, faire parler de soi dans les médias. Alors que convaincre ne serait-ce qu'une petite partie de la très importante communauté bitcoin de partir avec armes et bagages assure déjà le minimum ; cela garantit en outre une large couverture médiatique – le fork devient un événement de la vie du bitcoin et tous les médias en parlent. En outre, en vertu de la logique du fork, tous les détenteurs de bitcoins reçoivent des unités de cette nouvelle cryptomonnaie et peuvent la revendre ou la thésauriser (ceux qui détenaient des bitcoins au 1er août 2017 ont reçu le même nombre de Bitcoins Cash sur leur compte), c'est un cadeau en quelque sorte, une formidable publicité.

Ceux qui ont reçu des Bitcoins Cash (BCH) ont l'impression de toucher de l'argent qui tombe du ciel, mais il s'agit là d'une analyse à courte vue : le bitcoin se divise et donc il s'affaiblit (nous reviendrons sur cette idée). Si le fork n'avait pas eu lieu, le bitcoin vaudrait plus cher.

1. Selon le site de référence coinmarketcap.com.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

On peut légitimement considérer le fork comme une attaque contre Bitcoin[1] : le réseau bitcoin est inattaquable, nous le savons, copier son code pour créer une cryptomonnaie *ex nihilo* se révèle très ardu, donc on le « forke ». Scinder sa communauté assure une publicité mondiale gratuite, on récupère son nom et sa notoriété au passage (Bitcoin Cash, Bitcoin Gold, à qui le tour ?), et c'est très populaire puisque les détenteurs de bitcoins se retrouvent avec une nouvelle cryptomonnaie dans leur portefeuille et une impression de richesse supplémentaire. On espère que ce sera une mode passagère.

Une création originale

On ne copie pas le bitcoin, on ne le forke pas, on fait un vrai travail de création, d'entrepreneur. C'est le cas d'Ethereum et de la plupart des grandes cryptomonnaies.

Jusqu'en 2015, le bitcoin représentait plus de 90 % de la capitalisation totale, les autres cryptomonnaies se partageant les miettes. Mais 2017 marque un changement radical puisque le bitcoin passe sous la barre des 50 % (à partir du mois de juin). Désormais il faut compter avec de sérieux concurrents. Voyons quels en sont les principaux.

Les 15 plus importantes cryptomonnaies (18 janvier 2018)

Rang	Cryptomonnaie	Capitalisation (en milliards d'euros)
1	Bitcoin	152,6
2	Ethereum	78,6
3	Ripple	43,1

1. Une analyse que j'emprunte à Manuel Valente de La Maison du bitcoin.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

Rang	Cryptomonnaie	Capitalisation (en milliards d'euros)
4	Bitcoin Cash	24,2
5	Cardano	12,9
6	Litecoin	8,1
7	NEM	7,2
8	NEO	7,1
9	Stellar	6,8
10	IOTA	6,0
11	EOS	5,1
12	Dash	4,9
13	TRON	4,2
14	Monero	4,0
15	Bitcoin Gold	2,5

Source : coinmarketcap.com, 18 janvier 2018

Ce tableau regroupe les « coins », les cryptomonnaies proprement dites, et les « tokens », nés d'une ICO (voir le chapitre suivant), comme TRON. Le classement se fait par leur poids, leur valeur totale, leur capitalisation (nombre d'unités en circulation multiplié par leur cours). Avant de passer en revue ce classement, il faut noter deux éléments essentiels :

- sa forte volatilité : le bitcoin recule fortement à la mi-janvier, il passe quelques temps sous les 8 000 euros le 17 janvier, soit la moitié de son record atteint un mois plus tôt. L'ensemble des cryptomonnaies connaît une chute du même ordre de grandeur. Ces mouvements de cours sont tout à fait courants, il faut le savoir.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

- sa grande variabilité : un an plus tôt, le 15 janvier 2017, Cardano, Stellar, IOTA, NEO, TRON, EOS ne figuraient pas dans les 15 premiers. On notait la présence de MaidSafeCoin à la 8e position qui, à la date du 18 janvier 2018, est tombé à la 85e place, ou encore de Steem et Augur qui ont reculé respectivement à la 34e et à la 42e place. Il est fondamental de garder cet élément à l'esprit, notamment lorsqu'on investit. Des cryptomonnaies peuvent apparaître parmi les leaders puis sombrer ensuite dans les profondeurs du classement. Le site coinmarketcap.com recense plus de 1 300 coins et tokens avec de grosses capitalisations mais en nombre très limité (à partir du rang 6 on passe sous les 10 milliards d'euros), puis ensuite ce qu'on appelle une « longue traîne » contenant une multitude de valeurs d'un montant unitaire faible. Cependant la domination du bitcoin continue de s'effriter, alors qu'il représentait 55 % de la valeur totale des cryptomonnaies sur le second semestre 2017, il tombe à moins de 40 % en janvier 2018.

Ethereum

Ethereum est l'autre grande monnaie numérique (en fait Ethereum est le protocole et l'ether est la monnaie), celle qui pourrait peut-être supplanter le bitcoin un jour. Pour comprendre sa spécificité, il faut indiquer que le bitcoin a d'abord été lancé (en 2009) comme monnaie numérique, puis ensuite on a découvert l'intérêt que représentait la blockchain, tandis qu'Ethereum a fait l'inverse : il s'est lancé (en 2015) en mettant en avant sa blockchain, sans chercher à faire de l'ether une monnaie largement acceptée par les commerçants. Sa blockchain est plus facile à programmer que celle du bitcoin, elle offre plus de fonctionnalités, d'où son succès.

Selon son jeune fondateur, le Russo-Canadien Vitalik Buterin (né en 1994), Ethereum n'a pas pour objectif de concurrencer frontalement

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

Bitcoin, il s'agit plutôt de deux utilisations différentes et complémentaires de la blockchain : « La blockchain Bitcoin a été conçue spécifiquement pour les devises alors qu'Ethereum permet de créer tout type d'application. » Il veut faire d'Etherum la « colonne vertébrale » d'une multitude de « cyberentreprises autonomes décentralisées » nécessitant très peu de maintenance et de main-d'œuvre : « Les règles de fonctionnement d'une société commerciale, depuis les apports en capital des actionnaires jusqu'au planning du personnel, pourront être transcrites en algorithmes et incluses dans la blockchain. Tout sera géré et enregistré de façon automatique, fiable et transparente[1]. »

Cette cryptomonnaie très prometteuse et très ambitieuse connaît un sérieux bug en mai 2016 : une DAO (organisation décentralisée autonome), nommée « TheDAO », est créée afin de financer des projets. Le succès est au rendez-vous puisque 15 % de la totalité des ethers existants y souscrivent (160 millions de dollars à l'époque). Malheureusement, un hacker parvient à détourner un tiers de la somme collectée ! La communauté Ethereum se pose la question de savoir s'il faut « remonter en arrière » la blockchain (faire un *roll back*) afin d'annuler le vol pour récupérer la totalité des ethers, ou ne rien faire et accepter cette perte. Nous sommes ici au cœur de la « logique blockchain » : si l'on peut passer le film à l'envers et annuler une transaction particulière (ici le vol), quelle crédibilité accorder à Ethereum ? Qui ne dit que cette opération ne sera pas renouvelée pour telle ou telle raison ? La blockchain est conçue pour être infalsifiable mais dans ce cas, en l'occurrence, la décision d'une opération de réversibilité est prise et 85 % de la puissance de calcul sont mis en œuvre pour « effacer » ce vol. Toutefois, 15 % des mineurs refusent cette décision et font scission (ils font un fork) et lancent l'ether classique (symbole : ETC) parallèlement à l'ether d'origine (symbole : ETH) qui restera largement prédominant.

1. « L'ether, la future monnaie qui vaut déjà des millions », *Le Monde*, 7 octobre 2014.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

Le bitcoin, lui, n'a jamais connu une telle reprogrammation de sa blockchain (elle semble même tout à fait inconcevable quand on connaît un peu sa communauté), ce qui lui confère incontestablement une intégrité supérieure.

Quoi qu'il en soit, l'Ethereum poursuit sa route avec succès puisque tout un écosystème se développe autour de lui. Il faut cependant noter une différence fondamentale avec le bitcoin : le nombre d'ethers n'est pas limité. Il n'y aura jamais plus de 21 millions de bitcoins, nous le savons, alors que pour l'instant, il n'existe aucun mécanisme de limitation de la production d'ethers. Selon son fondateur, Vitalik Buterin, ce sera peut-être le cas à l'avenir, mais rien en la matière n'est encore décidé. On voit ici qu'Ethereum est en réalité beaucoup plus centralisé que Bitcoin, il dépend de décisions prises par l'équipe fondatrice, ce qui peut permettre plus de souplesse d'adaptation, mais qui est également source de fragilité.

Bitcoin et Ethereum sont tous les deux un couple monnaie/blockchain, ils s'attachent l'un et l'autre à développer une blockchain performante qui attire de nombreuses entreprises et ils possèdent un historique sérieux dans ce domaine. La première place dans les années à venir devrait se jouer entre eux deux. Les autres cryptomonnaies importantes se consacrant essentiellement aux paiements, il y a peu de chances que l'une d'entre elles puisse espérer mieux que la troisième marche du podium. Cela dit, des petits nouveaux commencent à apparaître, on mentionnera NEO, NEM (voir ci-après), et Tezos (nous le verrons dans le chapitre consacré aux ICO).

Ripple

Lancé en 2012, Ripple vise à permettre des transactions financières mondiales sécurisées, instantanées, presque gratuites, et de toute taille, il est de plus en plus utilisé par les banques comme infrastructure de

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

paiement, c'est un peu la « crypto des banques ». Les transactions sont vérifiées par consensus entre les membres du réseau plutôt que par le processus de minage, ce qui en fait une cryptomonnaie très centralisée (les adeptes purs et durs des cryptomonnaies considèrent que Ripple n'a pas sa place dans ce classement).

Bitcoin Cash

Bitcoin Cash est né d'un fork du bitcoin le 1er août 2017. Une partie de la communauté refuse la proposition Segwit, la jugeant trop timorée, et préfère augmenter la taille des blocs (de 1 à 8 Mo).

Le cours se traîne à environ 10 % de celui du bitcoin, mais avec l'échec de Segwit2x en novembre 2017, des mineurs mécontents se réfugient sur Bitcoin Cash dont le cours explose de 350 à 1 500 euros durant le week-end du 11 novembre, pour refluer ensuite.

Cette cryptomonnaie demeure à la troisième place. Elle semble essentiellement « poussée » par quelques mineurs et places de marché sans qu'un véritable écosystème n'émerge pour l'instant…

Cardano

Cardano veut devenir une plate-forme de contrats intelligents (*smart contracts*) avec les fonctionnalités les plus avancées. C'est un concurrent d'Ethereum.

Litecoin

Litecoin est la plus ancienne cryptomonnaie, avec Namecoin, née après le bitcoin – les deux sont apparues en 2011. Litecoin est une variation du bitcoin, ses transactions sont confirmées plus rapidement. Hormis son ancienneté et la notoriété qui lui est rattachée, on ne note pas d'avantage comparatif particulièrement saillant.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

NEM

NEM est une plate-forme fondée sur une blockchain, elle propose à ses utilisateurs des services de paiement, de messagerie, de création d'actifs, etc.

NEO

NEO a l'ambition de devenir « l'Ethereum de la Chine », il a récemment acquis une certaine notoriété en raison de sa collaboration avec les autorités de certification chinoises pour cartographier les actifs réels en utilisant sa technologie de contrat intelligent.

Stellar

Stellar est un système qui permet de transférer des devises « classiques » (euro, dollar, etc.) et des actifs rapidement, de façon sécurisée et à moindre frais.

IOTA

IOTA est un système de transfert de données et d'argent conçu pour l'Internet des objets.

EOS

Comme Cardano, NEM et NEO, EOS cherche à concurrencer Ethereum en proposant une blockchain facilitant les *smart contacts* et permettant une meilleure scalabilité[1].

1. Montée en puissance.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

Dash

Créé en 2012, Dash apporte à ses utilisateurs un anonymat complet : contrairement à Bitcoin, qui par nature permet à tout observateur extérieur de suivre les transactions de compte à compte (d'adresse à adresse) puisque la blockchain est publique, Dash propose un mode de transaction qui rend virtuellement impossible le traçage des envois et des réceptions de monnaie. Voilà une confirmation supplémentaire, pour ceux qui persistent à l'ignorer, que le bitcoin n'est pas anonyme, ou si peu, et que « l'argent sale » n'a aucun intérêt à l'utiliser.

Désormais, les trafics illicites vont-ils se précipiter sur Dash (ou Monero) ? La totalité des Dashs en circulation pèse un peu plus de 3 milliards d'euros, une somme ridicule à l'échelle de ces trafics, qui pourraient certes en profiter.

Il faut se rendre compte que ces monnaies anonymes offrent une vraie alternative dans les pays autoritaires ou dictatoriaux, car ce sont aussi des outils de défense des libertés fondamentales. De la même façon que Thor ou Darknet permettent à des citoyens vivant dans des régimes autoritaires de consulter des sites interdits, Dash ou Monero sont des outils d'échange qui passent sous les radars.

TRON

TRON permet à chaque utilisateur de publier, de stocker et de posséder librement ses propres données et, sous une forme autonome décentralisée, de décider de leur distribution, de l'abonnement et de leur diffusion. Il permet en somme aux créateurs de contenu de gérer eux-mêmes leurs publications.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

Monero

Concurrent de Dash, Monero (lancé en 2014) met également en avant son anonymat et l'impossibilité de tracer les transactions.

Bitcoin Gold

Bitcoin Gold est né d'un fork du bitcoin le 12 novembre 2017. Son objectif est de « redécentraliser » le minage en faisant en sorte que la validation des blocs se fasse avec des cartes graphiques et non des ASIC, un matériel nettement plus coûteux et de ce fait réservé aux gros investisseurs.

Les grandes catégories de cryptomonnaies

On voit ainsi émerger plusieurs catégories de cryptomonnaies[1] :

- Le bitcoin, le maître-étalon, à la fois monnaie et infrastructure (la blockchain) ;
- les monnaies alternatives au bitcoin qui mettent en avant la facilité à effectuer des paiements (Litecoin, Bitcoin Cash). Ripple est un peu à part, il s'agit de la « crypto des banques ». Ces dernières l'ont largement adoptée, notamment pour les paiements transfrontaliers ;
- les monnaies anonymes, qui mettent en avant l'anonymat des transactions : Dash, Monero ;
- les monnaies infrastructures, qui mettent en avant leur blockchain et où la cryptomonnaie ne constitue pas un but en soi mais un outil parmi d'autres. C'est le cas d'Ethereum, de NEO, NEM, EOS, Cardano, etc. ;
- les monnaies à usage spécifique comme TRON (gestion de contenu) ou – elles ne figurent pas dans ce classement – SiaCoin

1. « Quelles différences entre les crypto-monnaies ? » coin24.fr.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

(stockage informatique), Augur (marché de prédictions), Golem (supercalculateur décentralisé) qui proviennent d'ICOs (voir chapitre suivant).

Notons que la quantité totale d'unités monétaires en circulation varie selon les cryptomonnaies : pour le bitcoin, rappelons-le, nous en sommes à 17 millions avec une limite à 20 millions, mais pour le Ripple, nous en sommes à 38,7 milliards pour une offre totale de 100 milliards. Cette donnée est à prendre en compte, notamment lorsqu'on évalue les cours (ces éléments se retrouvent sur le site coinmarketcap.com).

Dans l'univers très concurrentiel des cryptomonnaies, copier ne sert pas à grand-chose, il faut jouer de ses avantages comparatifs, choisir un créneau et apporter le meilleur service utilisateur. Gageons que d'autres types de cryptomonnaies émergeront dans les années à venir.

Signalons d'ailleurs un nouveau type d'intervenants : les États et banques centrales. Dubaï, le premier, a lancé sa cryptomonnaie (Em-Cash) utilisable par les services gouvernementaux, la Russie a annoncé le lancement du CryptoRouble, la Banque centrale de Suède veut lancer le E-Krona, et d'autres pays envisagent de faire de même. Les cryptomonnaies ainsi créées sont indexées sur la monnaie nationale, il s'agit pour les banques centrales d'offrir un moyen de paiement supplémentaire, pas de permettre la spéculation. Quoi qu'il en soit, quelle reconnaissance pour les cryptomonnaies que de voir des banques centrales passer par elles !

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

Les ICO et les tokens, un nouveau placement

Un type de placement entièrement nouveau, cela n'arrive pas si souvent dans la vie d'un épargnant ! C'est pourtant ce qui se produit aujourd'hui avec les ICO et les tokens. Le phénomène est émergent, mais il importe dès maintenant de savoir de quoi il retourne. Expliquons les enjeux, les opportunités et les risques de ce nouvel objet financier encore largement non identifié.

ICO, token : les définitions

Le terme ICO (*iInitial Coin Offering*) fait référence à IPO (*Initial Public Offering*), le terme anglais pour désigner l'introduction en Bourse. À cette occasion, une entreprise lève de l'argent pour financer son développement, de nouveaux actionnaires entrent au capital et financent ainsi l'entreprise. Une introduction en Bourse permet aussi aux détenteurs historiques du capital de vendre sur le marché tout ou partie de leurs actions pour empocher une plus-value.

Dans l'ICO, ce qui est « offert » est un actif numérique échangeable contre des cryptomonnaies, que l'on nomme un « token » (jeton en français). Mais attention, le token n'est pas une part du capital de l'entreprise, comme c'est le cas lors de l'introduction en Bourse, il s'agit d'un droit d'usage du service de l'entreprise, d'un bon d'achat en quelque sorte. Si l'entreprise fabrique des sites Internet, l'acheteur de

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

tokens pourra lui commander un ou plusieurs sites. Mais ce n'est pas tout, car on n'a pas forcément besoin de ce que produit l'entreprise, on peut aussi échanger les tokens sur une place de marché contre des monnaies numériques, principalement des bitcoins. Il s'agit donc également d'un actif financier ! On peut, dans notre exemple, se dire que cette entreprise possède un business model particulièrement novateur dans la fabrication de sites Internet et que par conséquent, ses tokens prendront de la valeur avec le temps, et que l'on réalisera une belle plus-value en l'acquérant lors de l'ICO.

Un token est donc un objet numérique double : un bon d'achat de l'entreprise émettrice, et un actif financier. C'est bien sûr le second aspect qui intéresse le plus les investisseurs dans le monde, puisqu'il s'agit tout simplement d'un nouvel actif financier qui fait son apparition dans la gamme des placements.

Le token est en quelque sorte une monnaie privée émise par une entreprise. Ce procédé concerne pour l'instant essentiellement des start-up, des entreprises technologiques en phase de lancement, mais pourquoi ne pas envisager dans le futur son extension à des entreprises déjà installées et qui souhaitent lever des fonds pour franchir un nouveau palier ?

Précisons que dans une ICO, on ne lève pas des montants en dollars ou en euros mais en cryptomonnaie, principalement en bitcoins (qui sont traduits en dollars ou en euros par les médias, pour plus de simplicité), ce qui implique pour l'investisseur intéressé qu'il possède préalablement de la cryptomonnaie.

Les ICO n'existeraient pas sans la blockchain, ils se fondent dessus et ils répondent à la même logique, celle d'un fonctionnement décentralisé. Mais précisons que ce n'est pas la blockchain du bitcoin qui en profite mais celle de l'Ethereum : 90 % des ICO se font sur cette blockchain, celle-ci étant plus facile à programmer et offrant plus de fonctionnalités – d'où son succès. Les tokens sont émis en nombre limité et ils ne sont pas falsifiables, cette intégrité du processus étant

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

garantie par la blockchain : l'entreprise ne peut pas fabriquer et distribuer « en douce » des tokens, et il est impossible de fabriquer des faux tokens.

Compte tenu de leur succès, nous le verrons, nous pouvons d'ores et déjà dire que les ICO sont la première « killer application » de la blockchain.

Les avantages de l'ICO pour l'entreprise

Pour l'entreprise qui lève des fonds, l'ICO permet de s'affranchir des lourdeurs des levées de fonds traditionnelles, que ce soit le capital-risque (qui nécessite d'avoir des contacts et de présenter son projet à de nombreuses reprises, ce qui prend du temps), ou l'introduction en Bourse (un processus lourd et coûteux). Une ICO est rapide à mettre en œuvre, peu coûteuse, mais il faut tout de même prévoir un budget communication.

L'autre avantage fondamental est qu'il n'y a aucune dilution, les actionnaires lèvent de l'argent sans que leur part détenue dans le capital de l'entreprise ne diminue, puisque le token n'est pas une action. Et c'est mieux qu'un crédit bancaire, puisqu'il n'a pas à être remboursé.

Les avantages de l'ICO pour l'investisseur

À l'heure actuelle, il est difficile aujourd'hui pour un particulier d'investir dans une start-up, à moins d'être lui-même référencé comme capital-risqueur, ce qui nécessite des moyens financiers importants. Avec l'ICO, n'importe qui peut décider d'investir une somme modeste dans une start-up dont il croit au business model. L'ICO démocratise comme jamais auparavant le capital-risque, elle abolit la frontière entre les investisseurs professionnels et Monsieur Tout-le-Monde.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

Pour l'investisseur, un autre avantage de l'ICO est qu'elle permet d'entrer dès le lancement de l'entreprise. Des personnes ont certainement pressenti dès l'origine que Google ou Facebook allaient réussir, mais ne pouvaient pas investir dans ces sociétés, car il fallait pour cela passer par des fonds d'investissement ou des capital-risqueurs, milieu dans lequel il n'est pas facile de s'introduire ; pour investir, elles devaient attendre l'introduction en Bourse, quand ces entreprises avaient déjà connu le succès et la célébrité.

L'ICO permet d'ubériser les banques d'affaires et les grands fonds de capital-risque, passage quasi obligatoire pour toute start-up qui veut grandir. L'entreprise et l'investisseur sont directement mis en contact sur une plate-forme sécurisée, transparente et à faible coût de fonctionnement. Avec les ICO, le capital-risque et les banques d'affaires qui s'occupent des introductions en Bourse sont complètement ubérisés !

Selon Balaji Srinivasan, associé du fonds Andreessen Horowitz, « les ICO feront tomber la barrière entre investisseurs professionnels et acheteurs de tokens de la même façon qu'Internet a fait tomber la barrière entre journalistes professionnels d'une part, et blogueurs et utilisateurs de Twitter d'autre part. Internet a permis à chacun de devenir journaliste amateur. Désormais, des millions de gens vont devenir investisseurs amateurs. Tout comme pour le journalisme, certains réussiront extrêmement bien, et se serviront de leurs réussites pour entrer dans la ligue des investisseurs professionnels ». Réciproquement, on assistera aussi au mouvement inverse : « Tout comme utiliser Twitter est devenu pratiquement un passage obligé pour les journalistes, les investisseurs traditionnels se mettront eux aussi à acheter des tokens. »

Les frontières disparaissent également : nul besoin de posséder la nationalité américaine, ou de se rendre aux États-Unis pour investir dans une ICO de la Silicon Valley. Un projet africain pourra également

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

solliciter les investisseurs du monde entier, ce qui est très compliqué avec les procédures actuelles.

L'explosion des ICO lors de l'été 2017

Le nombre et le volume des ICO demeurent très faibles jusqu'au début 2017, hormis celles d'Ethereum en juin 2014 pour son lancement (18 millions de dollars récoltés) et en mai 2016 (« TheDAO »). Mais à partir de mai 2017, les montants levés dépassent 200 millions de dollars, 600 millions en juin, 300 millions en juillet ! Selon une étude de Goldman Sachs publiée en août 2017, les montants mensuels levés *via* les ICO surpassent depuis juin 2017 ceux levés par l'ensemble des entreprises Internet *via* le capital-risque. C'est une révolution dans le financement des start-up.

Ce résultat est dû à quelques ICO records comme Tezos, Bancor ou Status (voir le tableau ci-après). S'il y a évidemment une dimension bullaire, il s'agit aussi, plus fondamentalement, d'un changement de paradigme. Si les ICO ont dépassé le capital-risque, elles restent encore loin des IPO, les introductions en Bourse qui, elles, cumulent 22 milliards de dollars depuis janvier 2017. Mais le phénomène des ICO prend toutefois racine et se développe à toute vitesse : en 2016, une soixantaine d'ICO ont été dénombrées, mais elles sont plus de 2 000 en 2017.

Dans le tableau ci-après sont présentées les dix plus grandes ICO recensées en septembre 2017. On notera que la plus importante, Tezos, est dirigée par un Français, Arthur Breitman, même si sa société est domiciliée en Suisse.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

Les dix plus grandes ICO (en septembre 2017)

Sociétés	Montants levés en millions de dollars	Activités
Tezos	232	Concevoir une blockchain concurrente d'Ethereum
FileCoin	200	Service de stockage de données fondé sur la blockchain
Bancor	153	Simplifier la création de nouveaux tokens de manière à ce que n'importe qui puisse en créer
TheDAO	152	Financement d'Ethereum
Status	95	Messagerie et accès à des services payants, le tout fondé sur la blockchain Ethereum
TenX	84	Système de paiement
PressOne	82	Publication décentralisée de contenu
MobileGo	53	Plate-forme décentralisée de jeu
SONM	42	Superordinateur décentralisé
Basic Attention Token	35	Conception de Brave, un nouveau navigateur Internet

Source : icomentor.net
Note : on le rappelle, les montants ont été levés en cryptomonnaie, principalement en bitcoins ; ils ont été ici traduits en valeur en dollars.

Si l'on regarde la répartition des ICO par activité, on se rend compte que les infrastructures dominent largement, il s'agit ici de financer de nouvelles blockchains ou des protocoles (Tezos se positionne comme

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

un concurrent d'Ethereum), ce sont les fondations en quelque sorte. Ensuite, presque un quart des ICO concerne la finance (paiement, trading, services financiers), ce qui montre que ce secteur a bien perçu les avantages de ce nouveau moyen de financement. La formule consistant à dire que « la blockchain est l'Internet de l'argent » prend ici tout son sens. Viennent ensuite une multitude de secteurs (jeux, commerce, immobilier, santé, musique, etc.), ce qui montre que la blockchain va impacter l'ensemble de l'économie, mais que nous ne sommes qu'au début de cette révolution.

Quels sont les risques des ICO ?

Il faut cependant faire attention de ne pas se laisser emballer par ces chiffres grisants. Les ICO ne sont pas un placement miracle pour l'investisseur ou l'épargnant, elles comportent des risques qui sont à la hauteur des espoirs qu'elles suscitent. Dressons la liste des différentes menaces liées aux ICO :

- La foire aux arnaqueurs et aux incompétents : évidemment, le processus est tellement facile, il n'y a pas besoin de monter un épais dossier pour convaincre les banques ou le marché boursier, aucune autorité ne valide l'ICO. En conséquence n'importe qui peut monter un projet soi-disant prometteur, empocher l'argent et disparaître. De nombreuses arnaques se sont produites à travers le monde, et se produiront encore. Les adeptes du « prends l'oseille et tire-toi » ont trouvé là un nouvel outil très performant, n'en doutons pas. Au-delà de l'arnaque, des entrepreneurs incompétents peuvent aussi fourvoyer de bonne foi des investisseurs. Il faut revenir à une vérité de base : le métier d'investisseur ne s'improvise pas, il nécessite des connaissances, du bon sens, une capacité d'analyse, du temps, et d'accepter l'échec aussi, qui permet d'apprendre. Il ne

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

faut pas se laisser griser, même si les ICO apparaissent comme un nouvel eldorado.

- L'incertitude juridique : les ICO sont nées sans demander d'autorisation aux instances de régulation, elles se trouvent dans un « vide juridique » comme on dit. Il faut espérer qu'un minimum de réglementation se mette en place, de façon à éloigner les arnaqueurs, mais sans pour autant étouffer ce nouveau mode de financement.
- La volatilité : nous l'avons dit, les tokens émis sont échangeables sur une place de marché contre des bitcoins, ou des ethers (la monnaie de l'Ethereum), que l'on peut ensuite échanger contre des euros. L'investisseur doit donc jongler entre trois devises dont deux sont très volatiles ! Le cours du token peut monter, mais ce gain peut être effacé si le bitcoin baisse par rapport à l'euro…
- L'inégalité de traitement : contrairement aux promesses initiales, certaines ICO ne sont pas équitables. Des investisseurs peuvent passer avant les autres et empocher la plus grande partie des tokens proposés. Lors de l'ICO de Basic Attention Token, l'équivalent de 35 millions de dollars ont été levés en 24 secondes seulement, un investisseur empochant à lui seul un quart des tokens. Dans cette ICO, certains investisseurs ont payé 2 200 dollars de frais de transaction pour être servis en premier. Il existe des pré-ICO dans lesquelles des fonds d'investissement entrent avant la date de lancement, obtiennent des tokens avec une substantielle réduction, puis les revendent juste après. Ces modalités sont précisées dans l'ICO, l'investisseur devra en tenir compte.
- Lever trop d'argent : une ICO « trop » bien réussie amène un déluge d'argent sur l'équipe fondatrice qui peut lui donner une impression de facilité, et ralentir la mise en œuvre de son projet. Jusqu'ici, globalement, les montants levés par les ICO s'avèrent nettement plus élevés que par le capital-risque traditionnel, ce qui limite automatiquement la croissance de leur valorisation (l'investisseur paye trop cher).

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

Les points clés à regarder avant d'investir dans une ICO

Quelles sont les informations importantes à prendre en compte pour évaluer une ICO et éviter de tomber dans un piège ou une arnaque ?

- L'équipe dirigeante : il faut « googleliser » les dirigeants pour voir leur antériorité, leurs compétences, s'ils sont reconnus dans le milieu des cryptomonnaies.
- L'advisory board : les personnalités réputées dans la communauté blockchain sont très demandées pour figurer dans les « advisory boards » (conseil consultatif, les mentors du projet) des ICO. Le plus souvent, leur présence est un excellent signe, même s'il y a eu quelques arnaques dans ce domaine (des personnalités inscrites à leur insu).
- Le « White Paper » : un document, le « livre blanc », est écrit spécifiquement pour le lancement de l'ICO (comme pour une introduction en Bourse pour laquelle c'est prévu par la loi). L'entreprise explique son projet, son business model, pourquoi elle fait une ICO, comment sera utilisé l'argent. Il faut bien analyser ce texte, c'est l'élément crucial qui fera prendre sa décision à l'investisseur.
- Les modalités de l'ICO : comment se fait l'émission de tokens ? Combien sont créés ? Y aura-t-il de nouvelles émissions de tokens, ce qui fera perdre de la valeur à ceux créés initalement ? Tous les investisseurs sont-ils sur un pied d'égalité ?
- L'utilité du token dans le projet : à quoi sert le token dans le projet ? Il ne doit pas être uniquement un moyen de lever de l'argent, il doit s'insérer dans le business model.
- Les garanties juridiques : la société et le projet sont-ils garantis juridiquement, y a-t-il des juristes dans l'équipe ou des conseils extérieurs ?

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

- La réputation du projet : on fera un tour sur les forums de référence (cryptofr.com en français, bitcointalk.org en anglais) pour voir ce que l'on dit du projet. On pourra aussi consulter les sites de notation d'ICO, qui commencent à apparaître (icobench.com, icobazaar.com), mais en ne prenant toutefois pas leurs notes pour argent comptant.

On le voit, évaluer une ICO ne diffère pas fondamentalement d'une introduction en Bourse, il est toujours question d'un projet, d'une équipe, des modalités d'introduction sur le marché, et de la réputation. La différence c'est que le sujet est souvent très technique et qu'il nécessite souvent, mais pas toujours, de bien comprendre « l'économie-blockchain ».

Deux exemples : iEX.ec et DomRaider

En France, quelques ICO ont eu lieu, prenons le cas de deux importantes opérations :

- iEX.ec (cloud décentralisé) en avril 2017 (12 millions de dollars) ;
- DomRaider (rachat de noms de domaine tombés dans le domaine public) en septembre 2017 (56 millions d'euros).

La société lyonnaise iEX.ec est une plate-forme de cloud-computing distribué (exploitation de la puissance de calcul ou de stockage dans le cloud) fonctionnant sur Ethereum. Elle a été créée fin 2016, son ICO marquant son vrai démarrage. La start-up a annoncé le 19 avril 2017 avoir levé 10 000 bitcoins (son objectif maximal) en seulement trois heures. Les investisseurs ont reçu en échange des tokens dénommés « RLC » qui leur permettent d'accéder aux applications fournies par la société, ou de les revendre contre des bitcoins sur les places de marché.

Comment s'est comporté le cours du RLC ? Le token a été émis, c'est-à-dire proposé à l'achat, à un cours de 0,0002 bitcoin (1 bitcoin

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

= 5 000 RLC). Ensuite, l'évolution de son cours[1] montre une forte progression et un premier sommet le 1er mai 2017, avant de baisser, puis un nouveau sommet début juin 2017 (un quasi doublement du cours). Mais depuis, le cours du RLC exprimé en bitcoin n'a cessé de baisser pour passer sous son cours d'introduction. Cependant, comme sur la même période, le bitcoin a fortement progressé, le token exprimé en dollars a, lui, gagné en valeur. Voilà qui montre la complexité de ce type d'investissement puisqu'il faut jongler entre trois cours dont deux sont très volatils (le token et le bitcoin). Cela dit, en l'occurrence, il valait mieux garder ses bitcoins que d'acheter ce token à moins, grâce à un bon sens du trading, de tout revendre lors d'un des deux sommets.

La société DomRaider a, elle, été fondée en 2013 et est spécialisée dans le rachat de noms de domaine tombés dans le domaine public. DomRaider a souhaité lever des fonds pour créer une plate-forme décentralisée de vente aux enchères des noms de domaine, et potentiellement, de tout autre produit. Son ICO s'est étalée du 12 septembre au 11 octobre. Le token « DRT » était proposé au prix de 0,10 euro (mais il est coté en bitcoins). Au cours de l'ICO, 560 millions de DRT ont été proposés, tous ont été vendus, ce qui fait une levée de fonds de 56 millions d'euros. Son cours[2] a également baissé – il aurait mieux valu garder ses bitcoins.

Des polémiques sont nées à l'occasion de cette ICO. Tout d'abord, le montant total levé par DomRaider (56 millions d'euros), qui a été annoncé par le PDG de l'entreprise, n'était pas public, ce qui est normalement le cas. D'autre part, des sites de notation (ICObazaar, ICOBench) ont donné de très bonnes notes à cette ICO, mais sans en préciser les raisons. Enfin, 22 « advisors » sont mis en avant, mais personne ne connaît leur rôle exact : ont-ils tous réalisé une « due diligence » (vérifications qu'opère un investisseur en vue d'une transaction) digne

1. Voir coinmarketcap.com/currencies/rlc/.
2. Voir coinmarketcap.com/currencies/domraider/.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

de ce nom, ou certains sont-ils simplement rémunérés en échange de leur image, sans avoir à aucun moment étudié le projet ? Plusieurs personnalités reconnues du secteur de la blockchain en France ont formulé des reproches sur ce manque de transparence (voir ci-après leur appel à plus de transparence).

2018, l'année où les ICO entrent dans l'âge adulte ?

Certains spécialistes ont des avis très négatifs sur cette nouvelle « token-économie », comme Austin Hill, le fondateur et ancien CEO de l'entreprise blockchain Blockstream, qui affirme : « C'est une nouvelle bulle Internet qui se reproduit. C'est un bordel absolu, une foule d'arnaques illégales et immorales qui se produisent à grande échelle. Le marché entier dysfonctionne complètement à l'heure actuelle[1]. » Même la plus importante levée de fonds relève de cette catégorie selon lui : « Tezos a levé 240 millions de dollars pour un white paper ridicule, fou – je l'ai montré à des informaticiens et ils ont juste rigolé. Ils ont blagué sur le fait que des enfants de maternelle auraient pu l'écrire. » Il y a sans doute un peu d'exagération dans cette opinion, ce type d'avis n'est pas majoritaire, le succès des ICO en témoigne, mais il nous rappelle qu'il est nécessaire de garder un œil critique.

Incontestablement, une nouvelle économie est en train d'émerger, mais nous en sommes au tout début, il est encore difficile de prendre ses marques, de distinguer le bon grain de l'ivraie… À l'inverse de ce commentaire pessimiste, on signale que les ICO comptent depuis peu leurs premières licornes (Qtum et OmiseGO), c'est-à-dire des sociétés qui ont dépassé le milliard de dollars de valorisation.

On notera que la plupart des ICO essayent de se domicilier en Suisse, où la législation est très souple. À l'autre extrême, la Chine a interdit, dé-

1. Dans VentureBeat, le 29 août 2017.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

but septembre, les ICO sur son territoire, et a même obligé les ICO ayant déjà eu lieu à rembourser leurs investisseurs ! Ce mouvement brusque rappelle l'interdiction du bitcoin fin 2013, avant que la législation ne se fasse plus accueillante dans les mois qui ont suivi. L'empire du Milieu figure désormais parmi les places fortes au monde pour cette monnaie.

Entre l'extrême libéralité suisse et l'interdiction (temporaire) de la Chine, on semble s'acheminer vers une réglementation en termes de garde-fous : il ne s'agit pas forcément d'un texte spécifique, qui pourrait étouffer ce dispositif ou le faire fuir dans des pays plus cléments, mais l'obligation, pour les émetteurs d'ICO, de respecter un minimum la législation concernant les actions et les introductions en Bourse. Aux États-Unis la SEC (l'organisme de régulation de la Bourse) a estimé, fin juillet 2017, que les tokens donnant des droits à l'investisseur (droit de vote) devaient être considérés exactement comme des actions, ce qui implique un grand nombre d'exigences pour les porteurs de projet. Résultat, ce type de token se fait très rare. Si le token se rapproche d'une action, il perd sa dimension mondiale, et ce sont les législations nationales qui le régissent.

En France, l'AMF (l'organisme de régulation de la Bourse) semble hésiter entre une réglementation spécifique ou l'adaptation du cadre existant. Selon Franck Guiader, le directeur de la division FinTech, Innovation et Compétitivité de l'AMF : « Nous menons une analyse juridique au regard de la législation existante, pour voir dans quelle mesure ces opérations méritent d'être captées par un corps de règles existant ou s'il est nécessaire de prévoir des règles *ad hoc* plus adéquates[1]. » Si l'on en juge par l'accueil fait au bitcoin et à la blockchain, une adaptation du cadre existant devrait suffire et les ICO ne devraient pas être maltraitées en France.

En octobre 2017, plusieurs acteurs de la communauté blockchain en France ont signé un appel à plus de transparence[2]. Pour eux la situation

1. *La Tribune*, 18 septembre 2017.
2. « ICO : l'impératif de la transparence », *Medium*, 5 octobre 2017.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

actuelle n'est pas du tout satisfaisante : « Peut-on qualifier une levée de fonds d'*Initial Coin Offering* (ICO) alors même qu'elle ne respecte pas l'une des caractéristiques les plus fondamentales des technologies blockchain : la transparence ? Les cas de récentes ICO semblent indiquer que oui… À nos yeux, un seuil d'alerte est désormais franchi. » Nous sommes donc au tout début du phénomène, l'écosystème n'est pas encore en place.

Signe de maturation du secteur, le taux de réussite des ICO chute : de 80 % jusqu'en juin 2017, il passe à 40 % en juillet-août puis à 30 % en septembre-octobre. Il ne suffit plus de communiquer sur un projet disruptif pour empocher de l'argent, les investisseurs deviennent plus sélectifs, il faut s'en féliciter.

Faut-il investir dans les ICO ?

Finalement, on peut dire que l'ICO constitue un phénomène particulièrement novateur, qui va disrupter la levée de fonds traditionnelle, mais qu'à moins d'être très compétent dans ce domaine et de comprendre tous les aspects techniques de la levée de fonds, il faut se garder d'y investir des sommes conséquentes. On pourra, en revanche, « essayer pour voir », y consacrer des montants raisonnables en étant pleinement conscient du niveau élevé des risques. Il semble manquer aujourd'hui d'intermédiaires de confiance capables d'accompagner l'épargnant dans ses choix. Il faut cependant se tenir au courant de l'évolution de ce phénomène tout à fait passionnant et qui s'annonce potentiellement très intéressant. Il n'y a pas beaucoup de produits financiers aujourd'hui qui portent autant de promesses de rendement !

Un autre élément doit être pris en compte : il ne suffit pas d'évaluer si la valeur du token va augmenter en valeur absolue, mais si elle va progresser plus rapidement que le bitcoin. Si l'on achète des tokens en

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

vendant ses bitcoins, dont le cours est orienté à la hausse, cela vaut-il la peine ? Le token augmentera-t-il plus vite que le cours du bitcoin ? Voici la question à se poser, et ce critère devient extrêmement sélectif…

Quelques sites pour s'informer

Ce secteur étant en pleine évolution, voici quelques sites à consulter régulièrement. En français, le site de référence est incontestablement icomentor.net, très pédagogique pour parfaire ses connaissances.

Pour suivre les ICO en cours et à venir, on ira sur coinschedule.com, tokenmarket.net ou kickico.com, tandis que coinmarketcap.com/tokens/ permet de suivre les cours des différents tokens.

On pourra aussi faire un tour sur les forums cryptofr.com (en français) ou bitcointalk.org (en anglais). On signale des sites de notation d'ICO comme icobench.com ou icobazaar.com.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

pyright © 2018 Eyrolles.

La tokenisation de l'économie

Encore plus confidentielle (aujourd'hui) que les ICO, la « tokenisation de l'économie » avance à grands pas et va, elle aussi, bouleverser en profondeur nos économies.

Des tokens pour des biens existants

Avec les ICO, on a parlé des sociétés qui lancent un produit tout à fait nouveau, mais le token peut aussi servir à représenter de la valeur existante, c'est ce que l'on appelle la tokenisation de l'économie. On peut « tokeniser » de l'immobilier (un appartement en location), une voiture (en location), un brevet, un artiste, un sportif, etc., en fait tout ce qui génère des flux d'argent…

Par exemple[1], la société américaine Kexcoin a tokenisé une partie de son parc immobilier (d'une valeur totale de 120 millions de dollars), ainsi on peut désormais investir quelques euros sur le marché immobilier américain, ce qui était impossible jusqu'alors, car il fallait obligatoirement passer par des intermédiaires coûteux et engager une somme importante. Voici d'autres exemples :

- LAToken tokenise de l'immobilier, et aussi des contrats de prêts ;
- Science tokenise son portefeuille d'investissements dans des start-up ;

1. Ces exemples proviennent de la vidéo « Tokeniser : pour quoi faire ? » de la chaîne DMTrading sur YouTube, 28 octobre 2017.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

- Blackmoon Crypto tokenise des stratégies d'investissement ;
- Swissborg tokenise des solutions d'investissement de la banque privée ;
- TokenStars tokénise des joueurs de tennis, des joueurs de poker, des footballeurs, des artistes ;
- RecordGram tokenise des artistes chanteurs.

Ces tokens sont listés sur des places de marché spécifiques (on n'y trouve pas de cryptomonnaies), qui comportent différentes rubriques : immobilier, stratégies d'investissement, joueurs de tennis, etc.

L'intérêt pour l'investisseur

Désormais, n'importe qui peut investir dans n'importe quel produit, dans n'importe quel pays, n'importe quel argent, même une petite somme ! Il s'agit d'une révolution complète. Aujourd'hui, pour investir dans de l'immobilier à l'étranger, dans un fonds d'investissement, un *hedge fund*, il faut une mise de fonds significative. Ces services sont l'apanage des banques privées qui fournissent des services haut de gamme à leurs clients, et prennent de confortables commissions. Le commun des mortels n'y a pas accès.

Avec la tokenisation, ces investissements deviennent accessibles à tous. Il s'agit d'une ubérisation massive des intermédiaires financiers « haut de gamme » et d'une démocratisation de produits jusqu'ici inaccessibles au plus grand nombre. Nous sommes au tout début de ce basculement.

L'intérêt pour le créateur de tokens

Partons d'un exemple simple. Je possède un studio d'une valeur de 200 000 euros à Paris que je loue. C'est mon seul placement, l'essentiel de mon épargne. Pourquoi est-ce que je le tokeniserais ? En

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

tokenisant la moitié de mon studio, je perds la moitié des revenus qu'il génère, puisque je les verse désormais aux détenteurs de tokens. Sauf qu'à cette occasion, au moment de la tokenisation (de la mise sur le marché de ces tokens), je récupère 100 000 euros. Et donc je rends liquide quelque chose qui ne l'est pas. Sans cette tokenisation les 200 000 euros sont « bloqués » dans les murs.

Et investir 200 000 euros dans un studio, quand c'est toute l'épargne dont on dispose, constitue un choix risqué puisqu'il n'y a aucune diversification. Alors qu'après la tokenisation, je dispose de 100 000 euros que je peux investir dans des tokens immobiliers en province, en Allemagne, aux États-Unis, etc., et ainsi détenir un portefeuille immobilier réellement diversifié.

Le token de mon studio est coté, si je ne trouve pas de locataire, son cours va baisser et ma « réputation » aussi, ce qui bloquerait toute possibilité de développement futur, ce qui constitue une excellente motivation à être efficace.

La tokenisation permet de rendre liquide des actifs qui ne le sont pas ou peu, ce sont des masses d'argent gelées qui peuvent se réintroduire dans l'économie. La tokenisation permet également de rendre accessible des produits jusqu'ici réservés aux gros investisseurs, et donc d'étendre considérablement leurs débouchés. Les perspectives sont à peine imaginables.

Les risques

La tokenisation fait immédiatement penser à la titrisation, et c'est au fond la même chose puisque l'on crée des titres négociables à partir d'actifs peu liquides. Et la titrisation a très mauvaise réputation, ce qui n'est pas injustifié, loin de là : les *subprimes*, qui ont provoqué la crise financière de 2008, c'était de la titrisation (de prêts immobiliers).

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

Mais ce n'est pas tout à fait la même chose non plus : la titrisation se fait dans le secret des grandes banques, nous sommes dans la « haute finance ». C'est une « boîte noire » inaccessible à tout un chacun, et même en grande partie aux instances de régulation officielles. Alors que la tokenisation se fait sur la blockchain, avec des *smart contracts*, tout est transparent, et les commissions sont nettement moins élevées. Alors bien sûr, au début, il y aura des escrocs et des naïfs, comme on l'a vu pour les ICO jusqu'à l'été 2017, mais ensuite cette révolution devrait changer en profondeur notre économie.

Vers une « économie P2P »

Nous avons raisonné jusqu'ici à l'intérieur d'un secteur (l'immobilier dans notre exemple), mais la tokenisation peut concerner tous les domaines de l'économie, et les mettre en relation. Prenant l'exemple d'un particulier qui dispose de panneaux photovoltaïques, l'expert Pierre Paperon explique que, jusqu'ici, il ne peut que déverser sa production dans le réseau national, alors que désormais, « la blockchain permet de fabriquer ces unités plus petites que l'on peut appeler des "crypto-kWh" par exemple et qui ne sont rien d'autre que des kWh dont la production a été authentifiée par un compteur. Cela ouvre la voie à la vente au détail entre particuliers, mais aussi à une nouvelle ère de l'énergie *peer-to-peer* : l'énergie échangeable entre pairs, exactement comme Napster l'a fait en son temps pour la musique. »[1]

À partir de là, tout peut être tokenisé, le pot de miel, le kilo de carottes, un cours de mathématiques, sa voiture, des petits travaux de dépannage, et échangés entre eux de façon décentralisée. On va ainsi vers une sorte de « SEL 2.0 », pour Système d'échange locaux (SEL), dont plus de 400 existent en France et dont l'unité de compte est l'heure, quel que soit la nature du service. Les SEL permettent de

1. observatoire-blockchains.com.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

valoriser des compétences qui ne le seraient pas forcément dans le cadre économique classique, de créer de l'activité et des opportunités d'échange. Mais les SEL sont fermés, on ne peut pas échanger les unités d'un SEL à l'autre, ni les convertir en euros ; la tokenisation le permet.

C'est alors tout un nouveau pan d'activités qui devient possible pour une collectivité, les gains économiques seraient considérables : « les modélisations micro-économiques faites pour une commune de 1 000 personnes et en prenant des hypothèses raisonnables de participation (e.g. 3 à 7 % de taux d'utilisation de 10 % des voitures mises à disposition, 5 % des maisons en photovoltaïque, 2 % en solaire thermique, 1 % en biogazier, 10 ha de blé, 500 poules…) indiquent un nouveau flux financier créé d'environ un million d'euros par an. C'est dans les mêmes ordres de grandeur que le budget municipal d'une commune de 1 000 habitants. »[1] Imaginons ce que cela représente à l'échelle d'un pays…

1. *Ibid*.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

pyright © 2018 Eyrolles.

Un bitcoin à 100 000 euros ? Les causes de la hausse du cours

Comment expliquer la progression du cours du bitcoin ? Jusqu'où peut-il aller ? Tentons de répondre à ces questions.

Le paiement, première cause de la hausse du cours du bitcoin

La première cause de la hausse du cours du bitcoin vient de son usage comme moyen de paiement (et de virement). C'est un élément que nous pouvons avoir du mal à appréhender en Europe. L'euro fait l'objet de critiques, justifiées ou pas – c'est un autre problème –, mais malgré tout il s'agit d'une monnaie stable, qui ne subit quasiment pas d'inflation, dont le cours varie relativement peu par rapport aux autres grandes devises, et lentement, ce qui laisse le temps à chacun de s'y adapter, et d'autre part, chacun peut convertir la somme qu'il souhaite dans une autre devise. Cela nous semble naturel, évident, mais il s'agit en réalité d'un privilège assez rare dans le monde. Les Américains du Nord, les Australiens et les Japonais peuvent en dire autant, ensuite c'est plus compliqué. Les pays qui dépendent de matières premières, notamment du pétrole, voient leur devise chuter lorsque les cours se replient (Afrique, Moyen-Orient, Amérique

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

du Sud, Russie), de nombreux pays n'ont pas d'infrastructures de paiement modernes (Afrique), des monnaies sont manipulées par des pouvoirs interventionnistes (Venezuela, Zimbabwe, Argentine, etc.), des pays comme l'Inde font une « guerre contre le cash » pour obliger la population à se bancariser, et à payer ses impôts, et dans la plupart des pays de la planète, sévit un contrôle des changes plus ou moins strict.

En cas d'effondrement de la monnaie ou de contrôle des changes, souvent le dollar sert de seconde monnaie afin de faciliter les échanges (notamment en Amérique du Sud). Mais, justement, le bitcoin commence à se faire sa place. Par sa facilité d'utilisation, puisqu'il suffit d'un compte sur un smartphone, il permet d'effectuer des paiements sûrs et instantanés, et il franchit sans problème les frontières.

On note de plus en plus d'utilisateurs du bitcoin dans les pays qui subissent une forte inflation et une sévère dépréciation de leurs devises, comme l'Argentine ou le Venezuela. Au Nigeria, selon le site NewsBTC, plus de 100 000 marchands acceptent le bitcoin : face à un système de paiement peu développé et à une monnaie (le naira) à l'évolution erratique, les Nigérians sont en train de trouver une solution efficace ; ne doutons pas qu'ils seront suivis par d'autres, en Afrique et ailleurs.

En Inde, le gouvernement de Narendra Modi a décidé, en novembre 2016, de supprimer les billets de 500 et 1 000 roupies, soit 86 % du papier-monnaie en circulation (!), obligeant les Indiens à les échanger contre de nouvelles coupures de 500 et 2 000 roupies, et à justifier l'origine des sommes qu'ils apportaient dans les banques… L'objectif du gouvernement consiste à lutter contre l'économie souterraine afin d'augmenter les recettes fiscales. Entre la pagaille généralisée que cette mesure provoque dans tout le pays, la corruption qui repart de plus belle et les pénuries de billets, l'économie réelle souffre et tourne au ralenti. Comme on pouvait s'en douter, le bitcoin « est en train de remplacer à grande vitesse le liquide dans les transactions

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

immobilières[1] » et près de 70 % des agents immobiliers proposeraient ce service. Le bitcoin attirerait 2 500 nouveaux utilisateurs par jour.

En Europe ou aux États-Unis, le paiement en bitcoins relève plus de l'anecdote ou d'un esprit évangélisateur. Cependant, dans le futur, une perte de confiance dans la monnaie suite à une nouvelle crise financière de type 2008 ou le retour de l'inflation pourraient favoriser les paiements en bitcoins.

Le bitcoin permet de la même façon d'effectuer des virements transfrontaliers à moindre coût, nettement inférieurs aux circuits traditionnels (banques ou acteurs spécialisés). Dans ce cas, le bitcoin peut simplement servir d'interface (euros changés en bitcoins, qui sont envoyés dans le pays de destination puis immédiatement changés en monnaie locale), ou il peut être gardé en tant que tel si la monnaie locale n'inspire pas confiance.

Avec le paiement et le virement, voici déjà deux briques de base d'un service bancaire. Et la capacité à garder ses bitcoins sur un *wallet* (portefeuille) installé sur un smartphone fait office de compte courant. On estime que la moitié de la population mondiale n'est pas bancarisée, et l'usage exclusif du liquide constitue évidemment un puissant frein au développement économique. Et voilà comment le bitcoin permet de bancariser facilement des populations à l'écart des réseaux bancaires !

Au-delà du paiement et du virement proprement dits, c'est l'activité économique portée par ces services bancaires qui constitue un puissant moteur pour le bitcoin.

1. « Post demonetization, Bitcoins new "black" in property market », *Daily News & Analysis*, 23 novembre 2017.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

Le placement, deuxième cause de la hausse du bitcoin

Le bitcoin n'est pas qu'un moyen de paiement, c'est aussi un placement. L'un ne va pas sans l'autre, mais ce n'est pas automatique pour autant. Expliquons-nous. Ceux qui utilisent le bitcoin pour effectuer des transactions doivent, par définition, en détenir une certaine quantité (comme un compte courant dans une banque). Comme ils se rendent compte que le cours est globalement orienté à la hausse, ils en déduisent qu'il est judicieux d'y placer une partie de son épargne. Mais l'inverse n'est pas automatique : on peut choisir de détenir des bitcoins sans pour autant les dépenser. C'est le cas des Européens et des Américains notamment, pour qui le bitcoin constitue un nouveau placement intéressant, sans qu'il y ait d'intérêt à l'utiliser dans la vie courante. Les Chinois également thésaurisent la monnaie numérique.

Aux États-Unis, la première place de marché (Coinbase) a dépassé fin 2017 les 13 millions de comptes ouverts, ce qui représente près de 4 % de la population américaine. « Dans un sondage réalisé à l'automne par BlockChain Capital auprès de 2 000 personnes, 2 % des sondés déclarent détenir des bitcoins, une part qui double pour la classe d'âge des 18-34 ans, les "Millennials", la "génération Y" née avant l'an 2000, versée dans les nouvelles technologies et qui a trouvé dans le bitcoin une devise à son image, nomade, libre et décomplexée[1]. » Selon ce sondage, un Américain sur cinq envisage d'acheter des bitcoins dans les cinq années à venir, les Millennials de sexe masculin étant deux fois plus nombreux que la moyenne à l'envisager (41 %), tandis qu'à l'inverse, 80 % des plus de 65 ans ne souhaitent pas le faire ; l'enthousiasme à l'égard du bitcoin décroît avec l'âge. Les particuliers américains qui détiennent des bitcoins sont particulièrement optimistes sur

1. « Ces particuliers qui misent sur le bitcoin », *Les Échos*, 20 novembre 2017.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

ses perspectives : les deux tiers d'entre eux fixent à 200 000 dollars le cours à partir duquel ils céderont tout leur portefeuille[1].

Un élément fondamental se met en place qui va renforcer cette tendance : l'entrée en lice des institutionnels. En effet, il peut sembler un peu complexe pour les particuliers de se créer un compte sur une place de marché (un processus parfois un peu long), de faire un virement SEPA de leur banque pour alimenter ce compte, d'acquérir des cryptomonnaies, de les protéger. Ces démarches freinent la généralisation du bitcoin dans la population. Des acteurs institutionnels l'ont compris et proposent différentes solutions pour faciliter ces opérations :

- l'une des principales néobanques européennes, Revolut, a lancé fin 2017 la possibilité pour ses clients d'acheter et de vendre du bitcoin. D'autres devraient suivre ;
- TOBAM, une société parisienne de gestion d'actifs, a lancé en novembre 2017, le premier – un fonds commun de placement entièrement investi en bitcoins ;
- l'une des grandes places de marché américaines, Coinbase, a lancé fin 2017 un coffre-fort numérique pour les institutionnels ;
- en 2018, le Français Ledger lance « Ledger Vault » dédié aux entreprises et aux investisseurs institutionnels. Ces derniers (gestion de fortune, fonds d'investissement) pourront ensuite proposer l'achat de cryptomonnaies à leurs clients ;
- plusieurs grandes banques envisagent de proposer l'achat de cryptomonnaies à leurs clients (JP Morgan, Goldman Sachs…).

Au-delà, les fonds d'investissement (les *hedge funds*) s'intéressent de plus en plus aux cryptomonnaies – selon Reuters plus de 100 d'entre eux y étaient déjà investis en octobre 2017[2]. 2018 semble s'annoncer comme l'année des investisseurs institutionnels, et cet afflux constitue un puissant moteur pour la hausse du cours du bitcoin.

1. « Investing in Bitcoin : Survey & Report », lendedu.com, novembre 2017.
2. « Cryptocurrency hedge funds top 100 for first time », *Reuters*, 18 octobre 2017.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

La blockchain, troisième cause de la hausse du bitcoin

Nous l'avons vu, la blockchain permet d'implémenter différents services comme l'authentification de droits de propriété (en liant un document à une transaction précise), le paiement conditionnel (si tel événement a lieu, verser telle somme de tel compte à tel autre), l'échange de parts de capital de sociétés (et donc une bourse des valeurs), etc. Cette organisation décentralisée est plus efficace et moins coûteuse que les systèmes informatiques centralisés : un jour, peut-être, Airbnb et Uber seront ubérisés par des sociétés fonctionnant sur la blockchain… Des start-up se lancent sur ce créneau, le capital-risque afflue, les grandes banques s'y intéressent également, une quarantaine d'entre elles ont créé le consortium R3 pour développer des applications. Pour résumer, la blockchain, c'est un peu « l'Internet de l'argent », les potentialités sont énormes.

Bitcoin et blockchain, l'un ne va pas sans l'autre, mais nous avons affaire ici à plus qu'une monnaie : une technologie aux ressources insoupçonnées. Le développement des applications fonctionnant sur la blockchain renforce bien sûr le succès du bitcoin – voici une tendance de fonds poussant son cours à la hausse. Les ICO et la tokenisation n'en sont que les premières applications à succès, d'autres suivront.

Nous sommes au tout début du phénomène

On peut estimer fin 2017 le nombre d'utilisateurs et de détenteurs de bitcoins à environ 45 millions de personnes, soit entre 0,5 et 1 % de la population mondiale[1]. Ce chiffre correspond au taux d'adoption d'Internet au tout début, en 1994, lorsqu'il n'existait que seulement

1. « Les crypto-monnaies en 2017 : une situation identique à celle de l'Internet de 1994 ? », crypto-france.com, 28 novembre 2017.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

quelques milliers de sites. De cette époque, il ne reste quasiment que l'e-mail comme application populaire, les « portails », la grande affaire de l'époque, ont tous disparu (seul survivant : Yahoo !, grâce à sa messagerie). Et il faudra attendre plusieurs années pour que le commerce électronique s'implante vraiment, 2004 pour que Facebook et la mode des réseaux sociaux démarrent, etc. Avec Bitcoin, tout reste à écrire. Pour l'instant, l'ICO est la première « killer application » de la blockchain (de l'Ethereum), bien d'autres vont suivre.

Le taux de détention du bitcoin n'atteindra probablement pas celui d'Internet, c'est-à-dire de l'ordre de 95 %, mais si l'on inclut l'utilisation d'une technologie liée à la blockchain, on y sera sans doute. Nous sommes donc au tout début du phénomène, les perspectives de croissance sont gigantesques.

Un cours qui peut atteindre des sommets…

Essayons d'estimer ce que pourrait valoir le bitcoin lorsqu'il sera plus largement connu et utilisé. Et répondons par là même à la question lancinante : n'est-il pas trop tard pour en acheter ? Posons d'abord un principe d'analyse fondamental : il ne faut pas se focaliser sur le cours du bitcoin, mais sur sa capitalisation (son cours multiplié par le nombre de bitcoins en circulation), c'est-à-dire son poids réel[1].

Si l'on prend 17 millions de bitcoins produits (sur un total de 21) avec un cours de 10 000 euros, pour simplifier le calcul, le bitcoin pèse 170 milliards d'euros. C'est beaucoup pour une monnaie qui ne valait rien lors de son lancement le 3 janvier 2009, mais cela reste une tête d'épingle dans la masse des actifs financiers. Pour prendre l'or physique, les 166 000 tonnes existantes[2], avec un lingot à 35 000 euros, pèsent 5 810 milliards d'euros, soit 34 fois plus. Selon le *Allianz Global*

1. Que l'on peut voir, ainsi que les autres cryptomonnaies, sur coinmarketcap.com.
2. Estimation du *Thomson Reuters GFMS*.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

Wealth Report 2016, le total des actifs financiers dans le monde s'élève à 155 000 milliards d'euros, le bitcoin n'en représente donc qu'un 911e. Mais si sa part grimpe à 1 % (soit 1 550 milliards d'euros), son cours serait alors de 91 000 euros…

Alors, un cours de 100 000 euros serait-il envisageable ? Faisons le calcul : prenons 20 millions de bitcoins multipliés par 100 000 euros, cela donne 2 000 milliards d'euros. C'est tout à fait plausible. Cette somme est équivalente au bilan de BNP Paribas : si le bitcoin devait s'arrêter là, on ne pourrait même pas dire qu'il s'agit d'un succès, tout juste une belle réussite. Ainsi, 2 000 milliards d'euros seraient encore une toute petite part de l'épargne mondiale, un tiers de l'or existant sur Terre, la dette publique de la France, un dixième de la dette publique des États-Unis, en somme un compartiment important mais secondaire de la planète financière. Il y aurait donc encore du potentiel de croissance à ce niveau de valorisation.

Le bitcoin est une monnaie qui sert aux transactions, mais aussi à protéger un capital dans le temps, un actif de placement. Il faut donc l'évaluer en tenant compte de ces caractéristiques, pas simplement par rapport à la monnaie circulante (billets + comptes courants) mais aussi par rapport aux produits d'épargne pris globalement.

Il faut bien comprendre que le bitcoin n'est pas une action (une entreprise atteint toujours une limite), ni une matière première (un prix trop élevé fait chuter sa consommation), mais une monnaie. Si personne ne l'utilise (comme au début), elle ne vaut rien. Si elle devient une devise importante au niveau mondial, utilisée par des centaines de millions de personnes, pour des transactions comme pour la thésaurisation, son cours peut atteindre des sommets.

Mark Yusko, le fondateur du *hedge fund* Morgan Creek Capital Management, fait cette très pertinente remarque dans un tweet du 18 septembre 2017 : « Le seul vrai pari ? Savoir si le bitcoin allait véritablement pouvoir passer de 0 à 100 dollars – ce qui est déjà un vrai miracle. Mais passer ensuite de 4 000 à 40 000 dollars ou

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

400 000 dollars, ça, c'est facile[1] . » On prend ici le problème à l'envers : le miracle c'est l'invention du bitcoin puis son développement auprès des premiers geeks convaincus et la démonstration de sa fiabilité et de son potentiel, ensuite cette idée géniale ne peut que percer. En achetant du bitcoin, on investit dans un nouveau paradigme.

La loi de Metcalfe

Une autre analyse se fonde sur la loi de Metcalfe, énoncée par Robert Metcalfe, qui établit que l'utilité d'un réseau est proportionnelle au carré du nombre de ses utilisateurs. Autrement dit, la valeur d'un réseau va augmenter de manière exponentielle à mesure que le nombre d'individus qui y ont recours augmente. On l'a vu pour le téléphone fixe ; au moment de son apparition, le fait d'en posséder un n'apportait qu'une faible utilité à cause du peu de personnes raccordées, mais cette technologie est vite devenue indispensable lorsqu'elle s'est généralisée.

On peut aussi l'appliquer à Facebook : lorsque le réseau social ne comptait que 1 million d'utilisateurs, en 2004, il était valorisé 5 millions de dollars. Il passe le milliard de dollars de valorisation en 2006 avec 12 millions d'utilisateurs. En 2010, avec 600 millions d'utilisateurs, sa valeur totale s'élevait à 56 milliards de dollars. Lors de son introduction en Bourse en mai 2012, Facebook comptait 900 millions d'utilisateurs et était valorisé à plus de 100 milliards de dollars. Fin 2017, Facebook compte 2 milliards d'utilisateurs pour une capitalisation qui s'élève à 520 milliards de dollars[2].

Deux spécialistes ont appliqué la loi de Metcalfe au bitcoin, il s'agit de Tom Lee, cofondateur de la société de conseil FundStrat et Tim

1. « Pourquoi une prédiction à 1 million de dollars par Bitcoin n'est pas si farfelue », crypto-france.com, 20 novembre 2017.
2. *Ibid.*

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

Peterson, fondateur de la société de conseil Cane Island Alternative Advisors. Les deux montrent que les trajectoires de Facebook et celle du bitcoin suivent la loi de Metcalfe, et le premier prévoit un cours situé entre 20 000 et 55 000 dollars en 2022 tandis que le second prédit un cours à 48 000 dollars en 2022, des prévisions relativement proches[1].

La fin 2017 marque le début de l'effet réseau, aux États-Unis en tout cas avec des records à 100 000 ouvertures de comptes par jour pour Coinbase, l'une des principales places de marché du pays. On en est au niveau de Facebook en 2006 ou 2007, il reste donc plusieurs années de forte croissance…

On « découvre » le bitcoin comme on a découvert l'or

Formulons une hypothèse pour comprendre la progression du cours : on « découvre » le bitcoin comme on a découvert l'or comme moyen de paiement, il y a très longtemps. Les premières civilisations, l'Égypte et la Mésopotamie, connaissaient l'or, non seulement pour ses vertus décoratives, mais aussi comme réserve de richesse. La découverte de l'or comme réserve de valeur remonte donc à la préhistoire, pour laquelle nous n'avons aucune source écrite. Mais on peut imaginer qu'après la découverte du métal précieux, certaines personnes se sont convaincues qu'il pourrait servir pour l'échange, ce qui était tout à fait nouveau pour l'époque où l'on comptait en têtes de bétail (certainement la première monnaie) quand on ne faisait pas du simple troc. Le « débat » a eu lieu, certains moquant ces chercheurs d'or qui passaient leurs journées les pieds dans l'eau à recueillir des paillettes, considérant que rien ne remplacerait le bétail. Mais en l'espace d'une ou deux générations, l'or l'a emporté pour ne plus jamais quitter la place de « monnaie numéro un » pendant plusieurs millénaires.

1. *Ibid.*

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

La perte du statut monétaire de l'or, le 15 août 1971 lorsque Richard Nixon signe la fin des accords de Bretton Woods, apparaît comme un battement de cils à l'échelle de l'histoire humaine, qui va peut-être bientôt se refermer tant la croissance de la dette mondiale s'avère insoutenable. L'or retrouvera alors un éminent rôle monétaire. Mais aussi le bitcoin et d'autres cryptomonnaies. En tout cas, le débat a lieu entre les pour et les contre, mais si, comme nous le pensons, l'idée du bitcoin comme « or numérique » se répand comme une traînée de poudre, la croissance de son cours sera phénoménale.

C'est notre économie qui est une bulle !

On parle beaucoup de bulle pour le bitcoin, il y a incontestablement des effets bullaires, des effets de mode, il y aura des ajustements, des mini-krachs, mais prenons du recul : n'est-ce pas notre économie qui est une gigantesque bulle ? La dette mondiale (publique + privée) dépasse 324 % du PIB de la planète selon l'Institute of International Finance. Elle est actuellement soutenable parce que les taux d'intérêt sont bas, mais cela ne va pas forcément durer.

Pour dire cela, nous ne nous appuyons pas sur des experts auto-proclamés ou des analyses complotistes mais sur la très prestigieuse Banque des règlements internationaux (BRI), surnommée « la banque centrale des banques centrales », et qui a publié un sévère avertissement à l'occasion de la publication de son rapport trimestriel de septembre 2017[1]. Claudio Borio, le chef du département monétaire et économique de la BRI, n'y va pas par quatre chemins :

- Le monde ne s'est pas guéri de la dette : après la crise de 2008, « les niveaux de la dette mondiale en proportion du PIB ont continué d'augmenter. Le désendettement n'a pas vraiment eu lieu.

1. *BIS Quarterly Review,* septembre 2017.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

Là où les niveaux de dette privée ont, dans une certaine mesure au moins, diminué, la dette publique a pris le relais ».

- Les taux bas provoquent des bulles : « Tous ces éléments soulignent à quel point les prix des actifs semblent dépendre de l'extrême faiblesse que connaissent les rendements obligataires depuis très longtemps. [...] les cours des actions sont tendus. Les valorisations ne paraissent conformes aux références historiques qu'une fois pris en compte le niveau des rendements obligataires. »
- Le nombre d'entreprises zombies (qui survivent en s'endettant, profitant ainsi des taux zéro) ne cesse d'augmenter : « L'augmentation du pourcentage d'entreprises dont les bénéfices ne peuvent couvrir le service de la dette – les "entreprises zombies" – n'est pas de bon augure. »
- Les banques centrales sont coincées : « Il existe ici une forme de circularité risquant d'aboutir à un piège de la dette : la baisse prolongée des taux d'intérêt à des niveaux inhabituellement faibles, indépendamment du dynamisme de l'économie sous-jacente, crée les conditions compliquant le retour desdits taux à des niveaux plus normaux. »
- Et il faut s'attendre à des crises bancaires : « Les indicateurs avancés de difficultés potentielles dans les systèmes bancaires signalent l'existence de risques pour les années à venir dans un certain nombre d'économies avancées ou émergentes. »

Les taux bas prolongés constituent une erreur grave, ils provoquent des bulles sur les actifs, ils amèneront une nouvelle crise avec des faillites bancaires. Chacun est prévenu.

La BRI pointe aussi le risque du retour de l'inflation, qui demeure certes basse pour le moment, mais cela pourrait changer : « Dans ce contexte, il est d'autant plus important de comprendre "l'inflation manquante", car l'inflation guide l'action des banques centrales. Cela

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

rappelle *En attendant Godot*. Pourquoi l'inflation reste-t-elle résolument si faible, alors que les économies approchent ou dépassent les estimations de plein emploi, et que les banques centrales déploient des efforts sans précédent pour la soutenir ? Cette question à 1 000 milliards de dollars déterminera la trajectoire de l'économie mondiale dans les prochaines années ainsi que, selon toute probabilité, l'avenir des cadres actuels de politique publique. Il est préoccupant que personne n'en connaisse véritablement la réponse. » À force de rechercher l'inflation, les banques centrales risquent de faire sortir le monstre de sa boîte…

La plupart de ceux qui dénoncent le bitcoin comme une bulle sont confortablement installés aux postes de pouvoir de cette économie malade de la dette[1]. Rira bien qui rira le dernier.

Des changements d'échelle à prévoir ?

Nous avons parlé « d'or numérique ». L'or, tout le monde connaît, les 7 milliards d'habitants sur Terre savent ce que c'est, tandis que le bitcoin, aujourd'hui, seulement quelques millions de personnes l'utilisent, quelques dizaines de millions le connaissent, la marge de progression est donc énorme. Mais attention, son cours est volatil et il existe différents types de risques, nous allons y venir.

Ce que l'on peut dire, c'est qu'une progression régulière se met en place au fur et à mesure que les utilisations du bitcoin et de la blockchain s'étendent, avec quelques à-coups néanmoins. Mais de vraies ruptures, des changements d'échelle, pourraient intervenir si la confiance dans les grandes monnaies venait à s'éroder, que ce soit par un retour de l'inflation, une crise financière de type 2008, ou un grand pays qui ferait défaut sur sa dette (la dette publique du

1. Par exemple Jamie Dimon, le patron de JP Morgan, qui déclare en septembre 2017 que le bitcoin est une « fraude ».

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

Japon s'élève à 250 % du PIB…). On constate déjà le début de ce phénomène dans certains pays émergents en difficulté en Amérique du Sud (Venezuela, Argentine), ou en Afrique, mais s'il touchait le Japon, l'Europe ou les États-Unis, la croissance du cours du bitcoin deviendrait irrésistible.

Dans ce cas, la prévision d'un bitcoin à 1 million de dollars que font certains bitcoiners aurait du sens. Reprenons notre calcul précédent : 20 millions de bitcoins multipliés par 1 million d'euros, cela donne 20 000 milliards d'euros. Le bitcoin pèserait alors autant que la dette publique américaine actuelle. Un tel chiffre semble très difficilement concevable aujourd'hui dans le cadre économique que nous connaissons, mais en cas d'effondrement d'une ou de plusieurs grandes monnaies internationales (euro, dollar, yen, yuan), avec la ruine des épargnants et la défiance généralisée que cela impliquerait, il serait tout à fait envisageable.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

Les risques associés au bitcoin

L'investisseur doit prendre conscience des différents types de risques associés au bitcoin.

La concurrence des autres cryptomonnaies

Nous sommes dans un domaine extrêmement concurrentiel, des centaines de monnaies numériques existent et on peut tout à fait imaginer qu'une nouvelle devise apparaisse et supplante l'acteur historique. Jusqu'à il y a peu, le bitcoin dominait outrageusement le secteur des monnaies numériques. Il en représentait plus de 90 % de la capitalisation totale. Cette période est désormais révolue, et sa part est tombée autour de 50 %.

Le projet Ethereum affiche de grandes ambitions et un écosystème puissant se développe autour de lui. Il aspire à devenir la blockchain de référence, et c'est le cas dans le domaine des ICO. D'autres cryptomonnaies mettent en avant la facilité du paiement, d'autres encore l'anonymat. Rien ne garantit que le bitcoin reste le numéro un. Mais en restant dans le peloton de tête, il verra son cours de toute façon progresser, il n'a donc pas trop à s'inquiéter. Cette diversification du paysage doit encourager l'investisseur à diversifier son portefeuille, de façon à répartir les risques. Nous y reviendrons.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

Le bitcoin pourrait-il être dépassé techniquement, « ringardisé », et doucement sombrer dans les profondeurs du classement ? Il bénéficie de la plus grande communauté de développeurs, du plus grand écosystème, c'est-à-dire d'une capacité à réagir et à s'améliorer sans cesse. Il ne profite d'aucun monopole, il évolue dans un univers ultra-concurrentiel, ce qui lui interdit de se reposer sur ses lauriers. Un tel scénario ne pourrait se produire qu'en cas de graves crises de gouvernance, et à ce moment, tout le monde aurait à y perdre. La probabilité d'un tel scénario demeure donc très basse.

Les problèmes de gouvernance et les forks

Nous l'avons dit, on compte trois forks du bitcoin dans le second semestre 2017 (Bitcoin Cash, Bitcoin Gold, Bitcoin Diamond), et d'autres sont prévus (Bitcoin Silver, Bitcoin Unlimited, Super Bitcoin)…

Nous avons vu précédemment pourquoi il y a autant de forks du bitcoin : créer une cryptomonnaie à partir de rien se révèle très difficile. Il faut inciter des mineurs à faire « tourner la machine », recruter des utilisateurs, faire parler de soi dans les médias. Alors que convaincre ne serait-ce qu'une petite partie de la très importante communauté bitcoin de partir avec armes et bagages assure déjà le minimum, et garantit en outre une large couverture médiatique – le fork devient un événement de la vie du bitcoin et tous les médias en parlent. En outre, en vertu de la logique du fork, tous les détenteurs de bitcoins reçoivent autant d'unités de la nouvelle cryptomonnaie et peuvent les revendre ou les thésauriser (ceux qui détenaient des bitcoins au 1er août 2017 ont reçu le même nombre de Bitcoins Cash sur leur compte), un cadeau qui constitue une formidable publicité.

Le problème est qu'ainsi le bitcoin se divise et donc s'affaiblit. Si le fork n'avait pas eu lieu, le bitcoin n'aurait pas perdu des développeurs

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

et des mineurs, un certain nombre d'utilisateurs et au final un peu de sa valorisation.

Jusqu'à présent, ces forks ont convaincu peu de monde, les dommages pour le bitcoin sont donc tout à fait limités, à peine perceptibles. Mais l'importante modification (dénommée Segwit2x) prévue pour le 16 novembre 2017 et finalement abandonnée au dernier moment, s'avérait autrement plus dangereuse puisque 80 % des mineurs la soutenaient contre une infime minorité de développeurs. Un conflit si marqué aurait pu aboutir à un fork massif qui aurait déstabilisé le bitcoin. Rien ne dit que ce scénario ne pourrait pas se reproduire dans le futur, et effectivement aboutir. Plusieurs forks massifs aboutiraient à un « émiettement » du bitcoin, ce qui entamerait sérieusement son potentiel de hausse, et même sa présence dans le peloton de tête.

On peut toutefois se dire que la volonté d'agir par consensus et de ne pas se tirer une balle dans le pied évitera les forks massifs, et que la mode consistant à créer des forks mineurs pour avoir son quart d'heure warholien de célébrité finira par passer. D'ailleurs, signe d'énervement des grands acteurs, BitMEX, l'une des grandes places de marché dans le monde, a décidé de vendre les Bitcoins Cash de ses clients et de créditer leurs comptes en bitcoins. La plate-forme a déclaré « ne pas cautionner les hard forks litigieux ».

La difficile « scalabilité » du bitcoin

Derrière la plus grande partie de ces forks et de ces conflits de gouvernance se cache un problème de fond : la limitation du nombre de transactions par seconde. Le bitcoin peut supporter 7 transactions par seconde au maximum (contre plus de 20 000 pour le réseau Visa), ce chiffre doit obligatoirement augmenter pour permettre son développement. Lorsque les transactions s'engorgent, il faut augmenter les

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

frais pour être certain qu'elles soient validées, ce qui va à l'encontre du projet initial d'un système bon marché.

Les débats sur ce sujet sont très techniques. Certains suggèrent d'augmenter la taille des blocs de transaction (qui est limitée à 1 Mo dans Bitcoin), c'est ce qui a motivé le fork Bitcoin Cash du 1er août 2017 qui, lui, autorise des blocs de 8 Mo. Mais cette solution à elle seule ne peut suffire, et en outre elle favorise les gros mineurs et conduit à une centralisation du réseau, ce qui va à l'encontre du projet initial. D'autres suggèrent de faire des blockchains satellites à la blockchain principale pour traiter les petits montants. Le protocole Segwit a été adopté en août 2017 (sauf par Bitcoin Cash justement) et il devrait permettre d'améliorer les choses sur ce plan, notamment avec Lightning Network qui permet de créer des « canaux de paiement » entre deux ou plusieurs personnes et pour lesquels seul le solde sera inscrit dans la blockchain, ce qui l'allégera et autorisera globalement un bien plus grand nombre de transactions par seconde. Des solutions de scalabilité seront implémentées en 2018, mais ce problème reste crucial pour l'avenir du bitcoin, c'est un point à surveiller.

Cette scalabilité du bitcoin devrait aussi permettre de diminuer sa consommation électrique, très importante. Celle-ci a été estimée début 2017 à 3,8 milliards de kWh par an, soit la moitié de la production d'un réacteur nucléaire[1]. Selon une étude de novembre 2017[2], le bitcoin consomme plus d'électricité que l'Irlande. Cette énergie est nécessaire, elle le protège de la fraude. Le réseau n'étant contrôlé par aucune autorité centrale, il fonctionne grâce à ses mineurs qui résolvent des opérations complexes de vérification sur leurs ordinateurs. Cette intégrité a un coût. Il faut cependant moduler ce qui peut apparaître ici comme un désavantage : le réseau de paiement et la blockchain permettent de substantielles économies par rapport aux systèmes

1. « Quelle est la consommation électrique du réseau Bitcoin ? », bitcoin.fr.
2. « Le Bitcoin consomme plus d'électricité que l'Irlande », *Capital*, 28 novembre 2017.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

très centralisés qu'elles remplacent, il faudrait mettre les deux dans la balance, mais cela s'avère difficile à mesurer.

Une forte volatilité

Un autre risque est sa volatilité très importante. Elle fut extrême en 2013 (15 dollars en janvier, 1 108 dollars fin novembre avant de chuter), elle a tout de même diminué depuis, même s'il y a encore de sacrées montagnes russes, par exemple une chute de 4 000 à 3 000 euros environ en l'espace d'une semaine à la mi-septembre 2017 suite à l'interdiction des ICO en Chine ; mais le cours s'est rapidement redressé ensuite. La capitalisation encore limitée du bitcoin fait que la survenance impromptue d'un grand nombre d'acheteurs, ou de vendeurs, peut déstabiliser son cours.

Cela dit, ajoutons une précision importante : le bitcoin est, pourrait-on dire, « volatil à la hausse », car sur la longue durée il monte, incontestablement. Ce n'est pas le cas des devises qui, lorsqu'elles commencent à chuter, ont bien peu de chance de retrouver leur valeur d'antan. Le Vénézuélien n'a aucun espoir que sa monnaie retrouve son pouvoir d'achat d'avant la crise ! Lorsqu'une monnaie s'effondre, elle finit par disparaître complètement pour être remplacée par une nouvelle (l'Allemagne est sortie ainsi de l'hyperinflation de 1923). Le bitcoin évolue dans les deux sens et s'inscrit globalement clairement en hausse. Dans ce cadre sa volatilité n'est pas si inquiétante.

Cependant un élément pourrait accroître cette volatilité dans le futur, et plus que cela encore. Le 31 octobre 2017, le CME (Chicago Mercantile Exchange), la plus importante Bourse d'échange de marché à terme, a annoncé le lancement de contrats à terme en bitcoins. Cette nouvelle a été accueillie très favorablement dans la communauté, mais c'est sans doute une erreur, car ces contrats vont non seulement accroître la volatilité, mais aussi permettre les manipulations de cours,

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

comme on le voit depuis longtemps sur l'or. Des ventes massives d'or-papier cassent régulièrement les hausses du cours de l'or, les grandes banques commerciales faisant ici le « sale boulot » au service des banques centrales qui ne veulent pas voir le métal précieux trop progresser car cela affaiblit la crédibilité de leurs monnaies-papier. De la même façon des ventes de bitcoins-papier (ces fameux contrats à terme) pourraient freiner la hausse du bitcoin qui, lui aussi remet en cause les monnaies-papier.

Preuve que ce produit relève de la finance-casino typique de la grande banque : le contrat à terme, s'il arrive à échéance, sera réglé non pas en bitcoins mais en dollars. Un contrat à terme consiste à s'engager à livrer un produit à un prix donné à une date précise ; toutefois, il arrive rarement à échéance, l'intérêt consiste à s'en servir pour spéculer ou pour se couvrir contre une hausse ou une baisse de prix. Mais un contrat à terme en or ou en pétrole doit, si son échéance advient, livrer son « sous-jacent », c'est-à-dire de l'or ou du pétrole. Pas le contrat à terme sur le bitcoin, ce qui est une exception, et la porte ouverte à toutes les manipulations.

Le risque d'étouffement par les États

Il semble très peu probable que les États veuillent un jour interdire purement et simplement le bitcoin, la plupart lui ayant déjà fourni un cadre juridique favorable. Incarnant l'innovation, la technologie et Internet, les cryptomonnaies et la blockchain constituent de puissants vecteurs de croissance. D'autant que cette économie est très facilement délocalisable, un pays qui l'interdirait verrait simplement fuir à l'étranger ses entreprises spécialisées dans ce domaine.

Cependant, ce qui peut aussi se produire, c'est un étouffement progressif à coups de réglementations tatillonnes, de fiscalité confiscatoire et d'entraves aux projets trop disruptifs remettant en cause certaines

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

professions réglementées bénéficiant d'un fort pouvoir de nuisance. Des domaines dans lesquels les administrations excellent, on l'a vu en France avec les interdictions de Heetch et d'Uber Pop face aux menaces des taxis parisiens. Nombre d'innovations de la blockchain risquent de se heurter à un mur. Ce sera autant de perdu pour la valorisation globale des cryptomonnaies.

Au-delà, dans le cas d'une grave crise financière de type 2008 avec des faillites bancaires et un retour de l'inflation, il se produirait certainement un mouvement massif vers le bitcoin, la « monnaie saine ». Cela, l'État ne peut pas l'accepter, lui dont le pouvoir ne peut aller sans le contrôle de la monnaie. Nous entrerions alors dans une sacrée période de turbulences…

L'avis de l'Autorité des marchés financiers

L'Autorité des marchés financiers (AMF) est le régulateur des marchés financiers en France. Elle a notamment pour missions de veiller à la protection de l'épargne. Elle a publié une note sur le bitcoin en novembre 2017[1]. Elle rappelle que « Bitcoin est un investissement risqué [qui] repose sur un marché non régulé [et que] n'étant pas une monnaie ayant cours légal, vous ne disposez pas non plus des garanties offertes par les banques centrales ». Bien sûr, puisqu'il s'agit d'un réseau décentralisé, mais c'est aussi ce qui fait la force du bitcoin, des monnaies « trop » régulées par des banques centrales interventionnistes connaissent souvent de graves déboires.

La note rappelle la forte volatilité du cours et indique que « le Bitcoin s'adresse aux investisseurs avertis : un minimum d'appétence technique et financière est nécessaire afin de comprendre le protocole sur lequel il repose et ses risques ». Nous ne pouvons qu'approuver, c'est l'objet de ce livre, et l'épargnant, quel que soit le produit dans

1. « Investir dans le Bitcoin : prudence ! », amf-france.org, 15 novembre 2017.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

lequel il investit, doit consacrer du temps et de la réflexion avant de prendre ses décisions.

L'avertissement d'un acteur du secteur

Le site de référence bitcoin.fr publie régulièrement dans ses articles un avertissement qui résume une grande partie des défis auxquels doit faire face cette monnaie, nous le reprenons *in extenso* :

« Avant d'être un actif, Bitcoin est avant tout une expérience inédite, il est donc recommandé de ne pas y investir plus que ce qu'on peut se permettre de perdre. En outre, avant d'acheter des bitcoins, il faut être conscient que le projet n'est pas, à l'heure actuelle, à son stade final, même si les fondamentaux du protocole ne bougeront probablement plus. De nombreux travaux sont en cours pour améliorer la fongibilité, la sécurité et surtout la scalabilité "off-chain" du réseau qui ne pourra jamais, par dessein (pour garantir sa résilience et sa résistance à la censure) inscrire dans son propre registre qu'un nombre très limité de transactions. Enfin il faut être conscient, avant d'investir, que l'exceptionnelle puissance de calcul du réseau Bitcoin implique une dépense énergétique colossale et croissante, un nouveau défi auquel, si l'essor se poursuit, il faudra bien répondre tôt ou tard. »

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

Comment acheter des bitcoins ?

Comment concrètement acquérir des bitcoins et d'autres crypto-monnaies ?

Les places de marché

Au tout début, pour acheter et vendre des bitcoins, il était nécessaire d'installer la base de données des transactions (la blockchain) ainsi qu'un logiciel sur son ordinateur, une procédure relativement lourde et, de ce fait, le bitcoin est longtemps resté confiné aux « geeks », aux passionnés d'informatique. Cela a changé en 2012-2013, lorsque de nouveaux acteurs ont eu l'idée de s'intercaler entre l'internaute et le réseau bitcoin : les places de marché. Il suffit donc de créer un simple compte login/mot de passe sur l'un de ces sites pour pouvoir acheter du bitcoin.

L'AMF fait un salutaire avertissement dans sa note sur le bitcoin : « Différentes plates-formes d'échanges accessibles en ligne permettent d'acheter/vendre des bitcoins contre une monnaie fiduciaire comme le dollar ou l'euro : il est essentiel de vérifier la réputation et la fiabilité de ces sites[1]. » La meilleure réponse que l'on peut apporter consiste à se reporter au classement établi par le site bitcoin.fr[2], un des sites

1. « Investir dans le Bitcoin : prudence ! », amf-france.org, 15 novembre 2017.
2. « Acheter des bitcoins », bitcoin.fr, https://bitcoin.fr/acheter-bitcoin/.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

de référence dans le domaine : il est construit sur les déclarations de ses utilisateurs, un public technophile et utilisateur de longue date des cryptomonnaies. Les places de marché qui sortent en tête sont Kraken.com, Bitcoin.de, Bitstamp.net, Localbitcoins.com, Paymium.com, Bity.com, etc. Elles existent depuis quelques années et sont dignes de confiance.

Il existe plusieurs types de places de marché[1] :

- Les plate-formes de trading (Kraken, Bitstamp, Paymium) qui permettent d'effectuer des achats au prix du marché avec des commissions modestes. On vire ses euros *via* un virement SEPA ou par carte bancaire (plus coûteux). Ces plate-formes, qui tiennent des comptes en euros, doivent être adossées à un établissement bancaire agréé par l'ACPR (Autorité de contrôle prudentiel et de résolution, un organisme de régulation dépendant de la Banque de France). Les formalités d'inscription sont généralement assez exigeantes (carte d'identité, justificatif de domicile), mais elles répondent aux normes en vigueur ; c'est comme lorsqu'on ouvre un compte bancaire. Ce sont clairement celles-ci que l'on privilégiera.
- Les plate-formes de mise en relation entre acheteur et vendeur (Bitcoin.de, Localbitcoins). Les prix de vente sont souvent supérieurs à ceux du marché mais les moyens de paiements sont variés (espèces, mandat compte de La Poste, virement bancaire).
- Les points de vente à sens unique, où l'on ne peut pas vendre des bitcoins, mais seulement en acheter (Coinhouse). Ils acceptent parfois, moyennant des frais supplémentaires, les paiements par carte bancaire ou cartes prépayées.
- Les changes physiques (La Maison du bitcoin à Paris, seul cas en France pour l'instant). Ils acceptent la carte bancaire, prélèvent une commission assez substantielle, mais conseillent et accompagnent les néo-utilisateurs.

1. « Obtenir des bitcoins », bitcoin.fr.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

Les plus professionnelles et les meilleurs marchés sont les plateformes de trading. Concrètement, il faut créer un compte (avec carte d'identité et justificatif de domicile), puis envoyer ensuite la somme en euros que l'on souhaite changer en bitcoins ou autres cryptomonnaies *via* un virement SEPA. Celui-ci se fera en France pour Paymium, en Allemagne pour Kraken ou en Slovénie pour Bitstamp, même si ces deux dernières sociétés se trouvent à Londres. Cette procédure implique, la plupart du temps, de faire une demande préalable à sa banque pour pouvoir effecteur un virement dans ces pays, ce qui prend en général quelques jours. Une fois le virement effectué, on retrouve ses euros sur la place de marché, et l'on décide du moment opportun pour les changer en bitcoins. Celui qui voudra se faire assister dans ses démarches ira à La Maison du bitcoin.

Dans ce domaine, il existe beaucoup d'escrocs qui flairent le bon filon : ils montent des sites et partent avec la caisse. On se méfiera des sites récents et des offres trop généreuses pour être honnêtes.

De nouveaux intermédiaires

Les places de marché ont incontestablement démocratisé l'acquisition de bitcoins dans la population, mais cela ne peut suffire. Les « Millennials » ou « génération Y » (les personnes nées entre 1980 et 2000 en Occident) sont férues des nouvelles technologies et n'éprouvent aucune difficulté à les utiliser, mais ce n'est pas forcément le cas de tout le monde. Passer par des sites qui ne sont pas connus du grand public, qui n'existaient pas il y a cinq ans, quasiment tous en anglais, qui vous demandent votre carte d'identité, avec un processus d'identification parfois complexe, qui nécessite de faire un virement SEPA, par exemple vers une banque slovène (pour Bitstamp), voilà qui n'est pas évident pour tout le monde. De nouveaux intermédiaires doivent émerger.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

Des lieux physiques, comme La Maison du bitcoin à Paris, où le nouveau venu est aidé, permettent de toucher un public plus large. Des acteurs déjà installés entrent sur ce créneau, comme la néobanque européenne d'origine anglaise Revolut qui offre à ses clients la possibilité d'acheter des bitcoins – dans ce cas cela devient aussi simple que de souscrire un plan d'épargne. Gageons que d'autres néobanques s'y mettront, et peut-être aussi un jour des banques traditionnelles…

Avec les offres « corporate » que préparent les places de marché, les services de gestion de fortune, les conseillers en patrimoine pourront proposer les cryptomonnaies à leurs clients, en leur épargnant la gestion technique et administrative. Des fonds d'investissement consacrés aux cryptomonnaies mettront également les cryptomonnaies à la portée de beaucoup. Des projets de ce type ont émergé en 2017 et connaîtront un développement important en 2018.

Toutes ces nouvelles offres élargiront incontestablement le public adepte des cryptomonnaies. Mais comme elles se traduiront cependant toutes par des frais supplémentaires, on conseillera donc de faire l'effort d'aller sur les places de marché.

Obtenir des bitcoins en vendant des biens et des services

Que vous soyez un particulier ou une entreprise, rien ne vous empêche de vendre des biens et des services en bitcoins plutôt qu'en euros ! Il faut juste que l'acheteur soit d'accord. Ce type de transaction demeure encore tout à fait embryonnaire en France, contrairement à un certain nombre de pays émergents touchés par l'inflation, le contrôle des changes ou la dévaluation de leurs monnaies. Et puis compte tenu de la progression régulière du cours du bitcoin, il n'est pas évident de trouver quelqu'un qui veuille bien s'en délester !

Cela dit les paiements en bitcoins sont de plus en plus nombreux, certains détenteurs souhaitent prendre une partie de leurs bénéfices.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

De plus en plus de commerçants acceptent le paiement en bitcoins[1]. Les prix sont affichés en euros et convertis en bitcoins au moment de la transaction, l'euro reste la monnaie de référence, le bitcoin est encore trop volatil pour jouer ce rôle.

Avantage déterminant du logiciel libre, sur lequel est construit le bitcoin, tous les sites d'achat/vente/transfert de bitcoins sont interopérables. Pour envoyer de l'argent à une personne à partir de Paypal, il faut que cette personne possède un compte Paypal. Alors qu'avec un compte ouvert par exemple sur Paymium, on peut acheter un produit sur un site qui aura créé son compte chez BitPay. Les différents acteurs qui développent les usages du bitcoin ne sont donc pas en concurrence frontale mais font ensemble la promotion d'une nouvelle technologie. L'effet réseau jouant à plein, le décollage peut être très rapide.

Obtenir des bitcoins par le minage ?

Au tout début de l'histoire du bitcoin, un simple ordinateur de bureau permettait de miner, et donc de toucher de temps en temps les 50 bitcoins de récompense. Cette époque est révolue, la puissance de calcul nécessaire est devenue telle que des sociétés (on parle de « pools » de minage) acquièrent du matériel informatique spécifique (ASIC) en grande quantité uniquement dédié à cette activité. Le minage s'effectue désormais sur ce matériel généralement situé dans des centres de données climatisés ayant accès à de l'électricité à tarif préférentiel. Le minage est devenu une véritable industrie, pour la plus grande partie située en Chine. À destination des particuliers, « un certain nombre de sociétés proposent la location "on cloud" de matériel de minage. Ces propositions sont rarement rentables, quand il ne s'agit pas tout simplement de pures escroqueries », comme l'indique le site bicoin.fr. Méfiance donc.

1. Une liste existe sur le site bitcoin.fr, rubrique « dépenser ses bitcoins ».

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

Se méfier des arnaques

Tout ce buzz, cette hystérie même autour du bitcoin attire inévitablement les escrocs. Il faut se méfier. Nous en avons parlé pour les ICO, mais les cryptomonnaies ne sont pas à l'abri. « L'endroit du monde où les arnaques se diffusent le plus est l'Asie du Sud-Est, en particulier la Chine. La culture du jeu d'argent est très forte là-bas. C'est d'ailleurs pour cette raison que la Chine a une attitude sévère envers les cryptomonnaies. En Europe, il y a aussi des arnaques mais elles sont moins organisées qu'en Asie », assure Alexis Roussel, cofondateur de Bity, plate-forme d'échange de bitcoin et d'ether. « On met "coin" à la fin de n'importe quoi et on dit que c'est une cryptomonnaie alors qu'il n'y a rien derrière[1] », se désole Manuel Valente, directeur de La Maison du bitcoin. Il existe aussi de fausses places de marché qui partent avec l'argent des clients.

Signalons quelques indices permettant de repérer les arnaques[2] :

- des promesses de retour sur investissement stratosphériques ;
- des « packs » incluant du trading automatisé (gagnant à tous les coups, du genre « 1 % par jour ») et du minage ;
- des garanties quant au fait que « vous ne risquez rien » ;
- des achats en crypto-monnaies bloqués durant un certain temps sur la plate-forme ;
- des promesses d'obtenir les altcoins nées des forks du bitcoin (vous envoyez vos bitcoins sur le site, et vous ne les revoyez jamais) ;
- très peu d'information sur la plate-forme (entreprise, fondateurs, équipe).

1. « Les arnaques aux crypto-monnaies se suivent mais ne se ressemblent pas », journaldunet.com, 8 novembre 2017.
2. Nous nous inspirons ici de « Soyez vigilant – un message important de la Maison du Bitcoin et Coinhouse », Medium, 17 décembre 2017.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

La plus connue de ces escroqueries en Europe est Onecoin : créée en septembre 2015, elle a tout l'air d'une cryptomonnaie comme les autres, sauf qu'elle est fondée sur une pyramide de Ponzi, les clients étant rémunérés grâce aux fonds apportés par les nouveaux entrants[1]. Cette « monnaie » n'est échangeable sur aucune place de marché reconnue. Voilà qui aurait dû alerter, et faire fuir, tous les éventuels clients. On mettra aussi un drapeau rouge sur BitConnect qui est dénoncé comme une pyramide de Ponzi par plusieurs sites français, et aussi par Vitalik Buterin, le fondateur d'Ethereum[2].

1. *Ibid.*
2. « BitConnect, la plus grosse pyramide de Ponzi de tous les temps ? », journalducoin.com, 8 novembre 2017.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

pyright © 2018 Eyrolles.

Comment stocker ses bitcoins ?

Les bitcoins ne sont pas stockés à un endroit précis, mais dans la blockchain c'est-à-dire sur tous les nœuds du réseau à la fois. La question n'est donc pas de savoir où sont vos bitcoins (ils sont partout !), mais si votre portefeuille est bien protégé et si vous en possédez les clés d'accès. Dans ce domaine, le principal risque, c'est vous.

Restez discret

Le vol de bitcoins en s'attaquant directement aux personnes a déjà commencé. Les réseaux criminels sont toujours à la recherche de nouveaux méfaits, et le bitcoin ne pouvait pas leur échapper. Un homme d'affaires turc qui s'était vanté sur sa page Facebook de sa soudaine richesse s'est fait voler ses 450 bitcoins en octobre 2017 ; il a été kidnappé et violenté pendant 8 heures jusqu'à ce qu'il donne ses codes d'accès[1].

L'information que vous détenez des bitcoins doit être réservée à votre premier cercle familial et amical, pas au-delà. Il ne faut pas répondre à la question « Mais toi, tu possèdes combien de bitcoins ? » à un inconnu ou une vague connaissance. C'est comme si l'on vous

1. « Lorsque l'on possède des bitcoins, mieux vaut rester discret », crypto-france.com, 28 novembre 2017.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

demandait ce que vous avez sur votre compte en banque ! Il s'agit d'une sécurité minimale.

Pareillement, on déconseillera d'installer une application bitcoin sur son smartphone. En cas de vol, les voleurs pourraient revenir chez vous pour vous extorquer vos cryptomonnaies.

Un ordinateur et un antivirus à jour

Il importe avant toute chose de vérifier que l'ordinateur que l'on utilise pour acheter des bitcoins sur une place de marché est bien à jour et bénéficie d'un antivirus. Cette précaution minimale est nécessaire, il faut absolument éviter les malwares qui récupèrent les mots de passe…

Il faut en outre se garder des fausses applications pour smartphone que l'on peut trouver sur Google Play Store ou sur l'Apple Store, elles reprennent le nom et le design de places de marché connues à seule fin de récupérer les identifiants, puis de voler les bitcoins. Par exemple Poloniex, l'une des principales places de marché dans le monde, ne propose pas d'application, des petits malins ont donc fabriqué de fausses « Poloniex Official App » pour tromper les clients. Pour éviter tout problème, il faut partir du site Internet et suivre les liens qu'il propose.

Un *wallet* physique

Les « anciens » vous le diront : ne gardez pas vos bitcoins sur les places de marché. Il est vrai que nombre de premiers adeptes ont connu de tragiques expériences, au premier rang desquelles la faillite de Mt. Gox en février 2014, alors première place de marché au monde. Des milliers de personnes ont vu disparaître des dizaines, des centaines, voire des milliers de bitcoins, ce qui représenterait une véritable fortune aujourd'hui. La plate-forme a perdu, ou s'est fait voler, 850 000 bit-

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

coins – un procès est d'ailleurs en cours au Japon. D'autres places de marché ont connu le même destin funeste, soit en étant dévalisées par des hackers, soit parce que les fondateurs sont partis avec la caisse.

Désormais les grandes plate-formes connues au niveau international (Coinbase, Kraken, Bitstamp, etc.) disposent de moyens financiers nettement plus importants pour se protéger. Coinbase affirme que « 98 % des fonds de [ses] clients sont stockés hors-ligne », ce qui représente une vraie sécurité. Mais le risque demeure : plus la valeur du bitcoin augmente, plus les hackers vont déployer des moyens importants pour s'introduire sur ces plate-formes. Il vaut donc mieux aller au bout de la logique du bitcoin et détenir soi-même ses cryptomonnaies, alors que se reposer sur les places de marché s'assimile au modèle bancaire actuel : on fait confiance à un acteur extérieur qui peut faillir.

Il faut se créer son portefeuille, son *wallet* en anglais, de façon à avoir le contrôle sur ses cryptomonnaies. Il existe deux options :

- Les *software wallet* ou *hot wallet* : ces portefeuilles fonctionnent sur des smartphones ou des ordinateurs connectés à Internet. On télécharge une application et ils sont opérationnels, on peut envoyer ou recevoir des bitcoins ou toute autre cryptomonnaie. Ils sont faciles à utiliser mais n'offrent pas une sécurité optimale, parce qu'ils sont exposés aux virus. Selon une étude d'une société de sécurité, 90 % des applications mobiles liées aux cryptomonnaies comporteraient des failles de sécurité[1] ! Ces applications ne doivent donc servir qu'à transporter de faibles montants, de la même façon que l'on ne va pas mettre toutes ses économies dans son portefeuille.
- Les *hardware wallet* ou *cold wallet* : pour stocker des montants importants, on aura recours aux « portefeuilles matériels », au « stockage à froid ». Un *hardware wallet* est un appareil élec-

1. « Selon une étude, 90 % des applications mobiles liées aux crypto-monnaies comporteraient des failles de sécurité », crypto-france.com, 29 novembre 2017.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

tronique physique (qui se branche sur le port USB), un mini-ordinateur qui conserve les clés. On parle ainsi de « stockage à froid », c'est-à-dire en dehors du réseau Internet. Et même si l'ordinateur sur lequel est branché ce *wallet* est virussé, le hacker ne pourra pas accéder au portefeuille. Lorsqu'on l'installe, ce *wallet* génère une suite de mots que l'on prendra soin de noter : en cas de perte, il suffit d'en racheter un et de rentrer ce code de secours afin de récupérer ses bitcoins. Le *wallet* est en outre protégé par un code PIN, personne ne peut l'utiliser hormis l'utilisateur. La seule option pour les voleurs consiste à s'introduire dans le domicile de la personne, à mettre la main sur ce *wallet* et à la « faire parler ». D'où la nécessité d'être discret.

Ces *wallets* fonctionnent en complémentarité : le *hardware* pour stocker son patrimoine, le *software* pour un montant faible servant à des dépenses courantes. Le site bitcoin.fr donne les portefeuilles logiciels (*software wallet*) les plus connus[1] (Copay, Mycelium, Electrum, Bitpay, Blockchain.info, Coinbase, etc.) et les portefeuilles physiques les plus recommandés[2] (le Français Ledger Nano, l'Américain Trezor).

Le Ledger Nano S

Le Ledger Nano S (70 euros) est une création de La Maison du bitcoin et ce produit français est devenu l'un des leaders mondiaux dans son secteur. La très courte notice est en anglais, le texte s'affichant sur la Ledger Nano également, mais c'est de l'anglais basique et le site pour configurer sa Ledger Nano est en français (voir « Langages en bas de la page »), même si la rubrique FAQ est en anglais. Ce matériel ne marche qu'avec le navigateur Google Chrome, qui est le plus répandu,

1. « Recevoir, conserver et dépenser des bitcoins : les logiciels et les applications », bitcoin.fr.
2. « Les *hardware wallets*, portefeuilles matériels », bitcoin.fr.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

sinon il faudra l'installer sur son ordinateur. Les Parisiens peuvent se rendre à La Maison du bitcoin pour se faire aider, sinon on conseillera de visionner la vidéo qui lui est consacrée[1] ou l'article qui lui est dédié[2].

L'installation se fait très simplement : on connecte sa Ledger Nano à la prise USB, on crée son code PIN, on prend bien soin de noter la suite de mots qui permet de récupérer son portefeuille en cas de perte, on ouvre le navigateur Google Chrome sur lequel on télécharge les applications Ledger Wallet Bitcoin et Ledger Wallet Ethereum, et on peut ainsi effectuer des virements (l'interface des applications est en français). Pour récupérer les bitcoins que l'on a sur une place de marché, on clique sur « recevoir » et l'on obtient une « adresse bitcoin de réception » que l'on copie/colle sur le compte de sa place de marché dans la rubrique « withdrawal » (retrait), et c'est quasi instantané. L'opération est aisée et elle est vraiment à conseiller car c'est la façon la plus sécurisée pour garder ses cryptomonnaies, le meilleur moyen de ne plus s'exposer au risque de vol ou de fraude de sa place de marché.

1. « LEDGER WALLET : Comment sécuriser ses cryptos au maximum » sur la chaîne YouTube de CryptoNation.
2. « Comment sécuriser vos ethers avec un *hardware wallet* », ethereum-France.com.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

pyright © 2018 Eyrolles.

Quelle stratégie d'investissement ?

Faut-il acheter uniquement du bitcoin ? Certes non, même s'il s'agit de la principale cryptomonnaie. Voyons comment diversifier, dans quel horizon de temps se placer.

Investir dans les cryptomonnaies et pas ailleurs

De la même façon qu'investir dans l'or signifie exclusivement acquérir de l'or physique en nom propre, que tous les autres produits (ETF, mines d'or, or mutualisé) ne sont que des succédanés ou de potentielles escroqueries[1], investir dans les « cryptomonnaies » signifie en acheter en direct, point, et se détourner du minage, des « packs » ou autres produits exotiques et attrape-nigauds qui pullulent sur Internet. L'AMF le signale d'ailleurs très justement : « D'autres propositions d'investissement sur le Bitcoin peuvent vous être faites sur Internet, comme l'achat de packs de formation ou de "mining" ou encore un "mandat de gestion" sur actifs numériques. Prudence absolue[2]. »

1. Philippe Herlin, *L'Or un placement d'avenir*, Eyrolles, 2017.
2. « Investir dans le Bitcoin : prudence ! », amf-france.org, 15 novembre 2017.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

Certains peuvent vouloir faire du trading, vendre à la hausse, acheter à la baisse, passer d'une cryptomonnaie à l'autre, mais cela demande une vraie compétence, beaucoup de temps, et une saine compréhension du niveau de risque qui n'est pas donnée à tout le monde. On se méfiera encore plus des instruments à effet de levier, comme l'indique l'AMF : « Attention également aux effets de levier du CFD qui peuvent s'avérer d'autant plus dangereux avec un actif aussi volatil que le Bitcoin. Les CFD sur Bitcoin sont des produits spéculatifs hautement risqués. »

La hausse actuelle du cours du bitcoin semble pérenne, les forces à l'œuvre (développement de l'écosystème blockchain, hausse des transactions et de la thésaurisation) s'accroissent – malgré tout, cet investissement implique de ne pas avoir le mal de mer, de savoir regarder les tendances longues, et d'être conscient des risques que nous avons listés plus haut.

On l'a compris, il s'agit d'un investissement à long terme (plusieurs années). On investit dans un changement de paradigme, pas pour faire un profit en l'espace de six mois.

N'est-il pas trop tard pour en acheter ?

On investit dans un changement de paradigme, à long terme (plusieurs années) et, nous l'avons vu, le cours de 100 000 euros n'a rien d'irréaliste, donc non il n'est pas trop tard pour investir. Mais le succès n'a rien d'automatique, les risques existent, le bitcoin doit relever le défi de la scalabilité, des forks peuvent l'affaiblir, l'Ethereum ou d'autres cryptomonnaies peuvent le supplanter… Il faut acheter, et continuer à s'informer.

Il ne faut pas se positionner par rapport au cours lui-même, car acheter un seul bitcoin représente déjà une somme significative, mais par rapport à son épargne : de quelles liquidités je dispose dont je n'ai

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

pas besoin dans les années qui viennent, que ce soit 1 000, 5 000, 10 000 euros ou plus, et on investit.

Comment diversifier ?

On peut décider d'investir uniquement dans le bitcoin, la cryptomonnaie numéro un et la plus ancienne mais, comme tout investissement, il est utile de diversifier. On peut prendre comme référence la répartition du marché des cryptomonnaies lui-même : le bitcoin en représente 55 %, l'Éthereum *x* % (voir coinmarketcap), etc., donc on met 55 % de bitcoins dans son portefeuille, *x* % d'ethers, etc.

Cependant, reproduire le marché à l'identique n'est pas possible, il existe un nombre considérable de cryptomonnaies, la « longue traîne » est très fournie. On pourra donc surpondérer les principales. Autre élément fondamental, nous en avons parlé, le nombre d'ethers (la monnaie de l'Ethereum) n'est pas limité, contrairement au bitcoin (21 millions). Même si Vitalik Buterin, son fondateur, a dit qu'il en limiterait le nombre sans doute un jour, il n'y a rien de fait aujourd'hui, ce qui représente un point défavorable. On n'hésitera donc pas en conséquence à surpondérer le bitcoin.

Ensuite comment diversifier ? Nous l'avons vu plus haut, on peut classer les cryptomonnaies en plusieurs catégories :

- Le bitcoin, le maître-étalon, à la fois monnaie et infrastructure (la blockchain) ;
- les monnaies qui mettent en avant la facilité à effectuer des paiements : Litecoin, Bitcoin Cash, Ripple ;
- les monnaies anonymes : Dash, Monero ;
- les monnaies infrastructures, qui mettent en avant leur blockchain : Ethereum, NEO, NEM, EOS, etc.

Voici une façon de diversifier, répartir ses investissements dans différentes catégories, c'est-à-dire, outre le bitcoin, acquérir de l'Ethereum, du Ripple, Dash ou Monero, éventuellement NEO, NEM.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

On peut aussi opérer suivant la distinction valeurs sûres/outsiders/nouvelles venues[1] avec, dans le premier groupe le bitcoin, Ethereum, Ripple, Monero, dans le second Dash, Ethereum Classic, Nem. Concernant les « nouvelles venues », la liste s'allonge chaque jour ou presque, elle nécessite un effort soutenu d'informations, ce qui prend du temps, mais c'est dans cette dernière catégorie que l'on peut espérer réaliser de belles plus-values rapidement. Chaque cryptomonnaie est un projet en soi qui nécessite une bonne compréhension de son marché. Citons IOTA qui veut devenir l'interface de l'Internet des objets, Golem et Sonm qui récompensent ceux qui louent une partie de la puissance de leur ordinateur, Waves qui veut gérer les programmes de fidélisation, etc. Pour cela il faut suivre les sites d'actualités dont nous donnons une liste à la fin de l'ouvrage. D'ailleurs, sur l'année 2017, si le bitcoin a réalisé une très belle performance puisqu'il a vu son cours multiplié par plus de 11, il n'arrive qu'en 14e position[2] ! Les dix premières places sont occupées par Ripple, NEM, Stellar, Dash, Ethereum, Litecoin (nous en avons parlé plus haut dans le chapitre sur les autres cryptomonnaies), auxquels il faut rajouter Ardor (un concurrent d'Ethereum), Golem (un super ordinateur décentralisé), Binance Coin (une place de marché chinoise pour les cryptomonnaies) et OmiseGo (portefeuille numérique et paiement). Le fait de suivre de près l'actualité des cryptomonnaies et des ICOs peut se révéler très payant.

Dans le cadre d'une stratégie plus offensive, on peut garder la moitié ou les deux tiers de son portefeuille de cryptomonnaies en bitcoins et Ethereum (les valeurs sûres) et faire des paris plus audacieux sur les valeurs émergentes, en étant bien conscient que leur volatilité se révèle bien supérieure à celle du bitcoin…

1. « Les crypto-monnaies les plus prometteuses en 2018 » coin24.fr.
2. « Les cryptomonnaies les plus performantes en 2017 (le bitcoin n'en fait pas partie) » Capital, 2 janvier 2018.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

Les menaces sur les épargnants du système bancaire « classique »

Nous l'avons vu plus haut, ce n'est pas le bitcoin, mais plutôt notre économie qui est une bulle avec sa montagne de dette qui ne cesse d'enfler. Le risque sur le système bancaire s'avère ainsi très important et, comme s'il fallait prendre ses précautions, les gouvernements européens et la commission de Bruxelles ont mis en place deux dispositifs juridiques extrêmement menaçants pour les épargnants, et dont les médias ont peu parlé.

Premièrement il y a la directive BRRD (*Bank Recovery and Resolution Directive*) en vigueur en France depuis le 1er janvier 2016 et qui permet à une banque en situation de faillite de ponctionner les comptes de ses clients (comme cela s'est passé à Chypre en 2013). Seuls les comptes de plus de 100 000 euros sont officiellement concernés mais il est permis d'en douter, car il y en aura très peu (ceux qui sont au-dessus de ce chiffre ont ouvert plusieurs comptes pour passer en dessous). Et rappelons que Chypre a reçu une aide de 10 milliards d'euros de l'Union européenne et du FMI, ce qui a permis effectivement de ne pas toucher aux comptes de moins de 100 000 euros. Mais dans le cas d'un pays comme l'Italie, l'Espagne ou la France, il faudrait apporter des centaines de milliards d'euros pour permettre de ne pas toucher à ces comptes, or personne ne le fera.

L'objectif de cette directive consiste à éviter qu'une faillite bancaire dans un pays oblige l'ensemble des contribuables européens à payer. Il s'agissait de responsabiliser chaque État. Fort bien, mais alors pourquoi les épargnants devraient-ils payer les pots cassés ? En quoi sont-ils responsables ? Il aurait fallu prendre le problème autrement : réduire la taille des banques *too big to fail* (trop grosses pour faire faillite), obliger à la transparence sur les produits dérivés, séparer l'activité de dépôt de celle de marché, augmenter nettement le niveau des fonds propres, etc. Mais ces mesures heurteraient de plein fouet

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

le lobby bancaire, spécialement les banques françaises, si fières de leur modèle de « banque universelle ».

Seconde menace, la loi Sapin 2 votée en juin 2016, permet de bloquer les contrats d'assurance-vie (interdiction des retraits, arrêt du versement des primes) en cas de « crise financière ». Là encore, l'épargnant paye pour les erreurs de gestion des sociétés d'assurance-vie.

On le voit, la prochaine grande crise financière se réglera sur le dos des épargnants par des ponctions directes sur leurs avoirs. Dans ce cadre, les cryptomonnaies, mais aussi l'or physique et l'immobilier constituent des échappatoires, une façon de se débancariser afin de protéger son patrimoine. Ne l'oublions pas, le bitcoin est apparu (dans un article de recherche) à l'automne 2008 en réaction à la crise des *subprimes*, comme antidote à une monnaie manipulée par les banques centrales. Il nous sera très utile lors de la prochaine grande crise financière. On peut consacrer une part vraiment substantielle de son épargne aux cryptomonnaies.

Ce qu'en pensent les détenteurs

Le site bitcoin.fr a réalisé en novembre 2017 une enquête auprès de ses lecteurs[1] et s'il ne s'agit bien sûr pas d'un sondage au sens classique du terme avec un échantillon « représentatif de la population française », il permet d'évaluer les comportements de ceux qui détiennent du bitcoin. Le site a repris les mêmes questions que celles du site américain LendEDU, une place de marché dédiée aux prêts étudiants qui avait interrogé 564 Américains ayant un jour acquis des bitcoins, ce qui permet de comparer ; bitcoin.fr a obtenu 618 réponses.

À la question « lequel de ces énoncés décrit le mieux la raison pour laquelle vous avez acheté des bitcoins ? », 46,8 % des interrogés répondent que « Bitcoin est une technologie qui va changer le monde »

1. « Investir dans Bitcoin – Résultats du sondage », bitcoin.fr, 27 novembre 2017.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

(40,78 % des Américains), 24,5 % pensent que « Bitcoin est une réserve de valeur à long terme, comme l'or ou l'argent » (21,81 % des Américains), 18,7 % croient que « Bitcoin est sous-évalué et ne fera qu'augmenter » (14,01 % des Américains). Voilà qui traduit une très bonne connaissance de la nature du bitcoin.

Le montant détenu annoncé est de 0,60 bitcoin pour les Français et 0,45 pour les Américains. Il s'agit de chiffres médians (la moitié des personnes en détiennent moins, la moitié plus) et non pas d'une moyenne, qui serait plus élevée car un petit nombre en détiennent beaucoup. Le chiffre est plutôt bas, ce qui indique un grand nombre d'acquéreurs récents, essentiellement en 2017 quand le bitcoin coûtait quelques milliers d'euros et valait déjà cher.

La durée de détention prévue est de 1 à 3 ans pour 29,7 % des Français (39,54 % des Américains), de 4 à 6 ans pour 25,9 % (22,34 %), plus de 10 ans pour 25,6 % (16,49 %). C'est globalement du long terme, ce qui est intelligent, et qui correspond à la nature même du bitcoin qui constitue un changement de paradigme.

La sécurité de ses bitcoins n'inquiète pas 52,9 % des Français et 55,85 % des Américains ce qui, pour le coup, frise l'inconscience ! Les places de marché ne sont pas le bon moyen de protéger ses cryptomonnaies, nous le répétons.

Environ un tiers des Français et des Américains (33,3 % et 32,62 %) ont déjà revendu tout ou partie de leurs bitcoins, ce qui n'est vraiment pas judicieux. On répète qu'il s'agit d'un investissement à long terme.

Enfin à quel cours ces détenteurs seraient-ils prêts à vendre leurs bitcoins ? Quelque 100 000 euros pour les Français (prix médian, 187 022 euros comme prix moyen débarrassé des valeurs extrêmes) et 196 165 dollars (164 388 euros) pour les Américains. Des estimations relativement convergentes et plutôt judicieuses même si nous avons dit qu'à 100 000 euros, il y aura encore du potentiel.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

pyright © 2018 Eyrolles.

La fiscalité

Le bitcoin et les cryptomonnaies en général sont bien sûr soumis à la fiscalité, voyons comment[1].

Les principes de base

Rappelons d'abord que le bitcoin n'est pas une monnaie ayant cours légal. On peut donc refuser un paiement en bitcoin sans contrevenir aux dispositions de l'article R. 642 du Code pénal. Seul l'euro a cours légal en France bien entendu, le bitcoin est à ce titre une « monnaie complémentaire ». Il faut que les deux cocontractants, l'acheteur et le vendeur, soient d'accord pour l'utiliser.

Les cryptomonnaies ne sont pas considérées par l'administration fiscale comme un revenu du capital (et donc taxées comme des valeurs mobilières) mais comme un revenu d'activité, en l'occurrence une activité spéculative, donc soumise à l'impôt sur le revenu. Et cette activité est soit occasionnelle, soit régulière.

1. Les éléments qui suivent doivent beaucoup aux interventions de Christophe Billet de DS Avocats et de Guillaume Lucchini de Scala Patrimoine lors de l'ICO Conférence du 9 novembre 2017 à Paris organisée par Largillière Finance, à l'article « Le bitcoin et la fiscalité » sur cryptogains.fr ainsi qu'à la vidéo de Hasheur sur YouTube « Bitcoin et Altcoins : droit, législation et fiscalité. Que devez-vous déclarer ? ».

Copyright © 2018 Eyrolles.

S'il devait entrer dans le calcul de l'ISF (impôt sur la fortune) au titre d'élément du patrimoine, ce n'est plus le cas avec l'IFI (impôt sur la fortune immobilière) qui le remplace depuis le 1er janvier 2018.

La TVA ne s'applique pas, selon une décision de la Cour de justice européenne (CUJE) du 22 octobre 2015.

On ne déclare qu'en cas de bénéfice

Dans le cadre de la lutte contre le blanchiment, en cas de revente et de conversion en euros, un montant important sera susceptible de faire l'objet d'un signalement Tracfin par votre banque. Il est donc nécessaire de conserver la trace de ses opérations (justifier que l'on a acheté tant de bitcoins à telle date et à tel cours). Les places de marché gardent l'historique de vos mouvements. Il importe donc de maintenir son compte actif de façon à pouvoir y accéder, même si l'on a transféré tous ses bitcoins sur un portefeuille physique. On gardera aussi la trace des virements que l'on a effectués de sa banque vers la place de marché.

Deux principes de base doivent être retenus :

- on n'a pas à déclarer ce que l'on possède comme cryptomonnaies ;
- on déclare uniquement quand on vend, et l'on déclare les bénéfices.

Lors d'une revente avec un bénéfice donc, que l'on soit un particulier, une profession libérale, un entrepreneur individuel ou un microentrepreneur (ex-autoentrepreneur), on est soumis soit aux BNC (bénéfices non commerciaux), soit aux BIC (bénéfices industriels et commerciaux).

L'imposition des gains dépend de ce que ceux-ci relèvent d'une activité occasionnelle ou d'une activité habituelle :

- activité occasionnelle : l'imposition se fait au titre des BNC (bénéfices non commerciaux) ;

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

- activité régulière : l'imposition se fait au titre des BIC (bénéfices industriels et commerciaux).

Concernant la distinction entre activité occasionnelle et activité habituelle, il faut noter que :

- l'absence de caractère professionnel de l'activité est sans incidence sur son caractère imposable (CE 19 février 2014, n° 354380). Autrement dit, on ne peut pas se retrancher derrière le fait que l'on n'est pas une entreprise pour s'imaginer que l'on ne tombera pas dans la catégorie « activité habituelle », si les achats et les ventes sont réguliers ;
- des opérations peu nombreuses mais périodiques peuvent caractériser une habitude, et donc l'imposition au titre des BIC ;
- selon l'avocat Olivier Martin sollicité par le youtubeur Hasheur[1], si les gains provenant de la vente des cryptomonnaies dépassent 50 % des revenus, ils sont automatiquement basculés en BIC. Voilà qui pose un sérieux problème, car avec la forte croissance de son cours, la revente de quelques bitcoins pourrait suffire à franchir ce seuil…

Lorsque le montant annuel des ventes n'excède pas 70 000 euros[2], le contribuable peut opter pour le régime des micro-BNC ou des micro-BIC :

- le revenu imposable au titre des micro-BNC est calculé après application sur le montant des ventes d'un abattement de 34 % représentatif des frais ;
- le revenu imposable au titre des micro-BIC est calculé après application sur le montant des ventes d'un abattement de 50 % représentatif des frais.

1. « Bitcoin et Altcoins : droit, législation et fiscalité. Que devez-vous déclarer ? », YouTube.

2. Plafond applicable depuis le 1er janvier 2017 selon le projet de loi de finances pour 2018.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

Lorsque le montant annuel excède le seuil de 70 000 euros, le revenu imposable est déterminé selon le régime réel pour lequel on notera l'application d'une majoration de 25 % au gain réalisé en l'absence d'adhésion à un centre de gestion agréé (CGA) pour les BIC ou une association de gestion agréée (AGA) pour les BNC. La première adhésion doit se faire dans les cinq premiers mois de l'année. On aura dont la précaution d'adhérer dans les cinq premiers mois de l'année de la cession de tout ou partie de ses bitcoins et autres cryptomonnaies.

Finalement, la facture fiscale peut s'avérer salée si l'on est concerné par les tranches les plus élevées de l'impôt sur le revenu (45 %). Et à ce taux il faut rajouter les prélèvements sociaux sur les revenus d'activité (CSG/CRDS) soit 9,7 %. Comme les cryptomonnaies ne sont pas considérées comme des valeurs mobilières, il n'existe pas d'abattement lié à leur durée de détention, et elles ne bénéficient pas non plus du prélèvement forfaitaire unique (la « flat tax ») de 30 %. Enfin, elles sont bien sûr soumises aux impôts sur les donations et sur les successions.

Il n'y a pas (pour l'instant...) d'« *exit tax* » : le transfert du domicile fiscal hors de France entraîne l'imposition des plus-values latentes sur les valeurs mobilières, mais l'article 167 bis du Code général des impôts ne mentionne pas les bitcoins. Voilà qui pourrait inciter ceux qui veulent réaliser de gros bénéfices à quitter la France.

Comme on le voit dans bien d'autres domaines, la fiscalité confiscatoire de la France va faire fuir les patrimoines importants... Il faudrait au moins considérer les cryptomonnaies comme des valeurs mobilières, ce qui allègerait la note.

On notera d'ailleurs que le 10 janvier 2018 à Lyon, le porte-parole du gouvernement, Benjamin Griveaux, a déclaré « qu'il n'y a pas de raison que la flat tax [de 30 % NDLR] ne s'applique pas aux cryptomonnaies ». Une avancée intéressante mais qui reste à confirmer.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

La législation pourrait devenir plus intrusive si l'on en juge par cette initiative du fisc américain qui a demandé, et obtenu devant un tribunal, en novembre 2017, que la principale place de marché américaine, Coinbase, lui communique les coordonnées de ses clients ayant échangé plus de 20 000 dollars de bitcoins au cours de la période allant de 2013 à 2015. Constatant que moins de 1 000 Américains avaient déclaré des gains sur le bitcoin entre 2013 et 2015, le fisc a décidé d'aller chercher ces informations directement sur les places de marché…

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

pyright © 2018 Eyrolles.

Des sites pour s'informer

On l'a compris, les cryptomonnaies sont un domaine en perpétuelle évolution, on ne manquera donc pas de mettre quelques sites dans ses favoris afin de se tenir informé.

On commencera par ces cinq sites d'actualités incontournables :

- bitcoin.fr
- journalducoin.com
- crypto-france.com
- coin24.fr
- cryptoactu.com

Le site de référence pour la cotation des cryptomonnaies et des tokens : coinmarketcap.com

Pour compléter ses connaissances sur le bitcoin on ira sur :

- bitconseil.fr
- bitcoin.org

Pour compléter ses connaissances sur la blockchain on ira sur : blockchainfrance.net

Pour compléter ses connaissances sur l'Ethereum on ira sur : ethereum-france.com

Pour un panorama didactique sur les cryptomonnaies, on consultera : cryptoencyclopedie.com

Pour des analyses tournées vers l'investissement, on ira sur : crypto-analyse.org

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

On consultera ces chaînes YouTube :

- Hasheur
- CryptoNation
- ainsi que les chaînes des sites d'informations cités précédemment (bitcoin.fr, Journalducoin, Crypto France, Crypto Analyse TV)

Pour des rencontres dans le « monde réel », on ira à La Maison du bitcoin (lamaisondubitcoin.fr) à Paris (certains de ses événements sont retransmis sur Facebook Live) et l'on s'inscrira sur Meetup, la plate-forme préférée des bitcoiners – Paris Bitcoin Meetup, Meetup Blockchain(s), Ethereum Paris, plusieurs groupes existent en province.

© Groupe Eyrolles

Copyright © 2018 Eyrolles.

Conclusion

Que conclure sur le bitcoin et les cryptomonnaies ? Nous ne sommes qu'au début du phénomène, comme l'époque d'Internet en 1995, il importe de bien comprendre les bases, les enjeux, les risques et les opportunités. L'essentiel reste à créer, mais pour cela il ne faut pas perdre un certain esprit frondeur du début ainsi que la volonté de diffuser une innovation positive pour le plus grand nombre. À cet égard, si certains bitcoiners publient des vidéos pour se vanter de la voiture qu'ils ont pu s'acheter, d'autres font preuve d'une certaine hauteur de vue, par exemple en partageant une partie de leur plus-value avec des œuvres de charité comme PineappleFund, qui fait don de 5 057 bitcoins : « Aujourd'hui, je vois qu'1 BTC vaut 17 539 $. Parfois, je n'arrive pas à y croire. Bitcoin a changé ma vie, j'ai plus d'argent que je ne pourrai jamais en dépenser. Mes buts, ce qui me motive dans la vie n'ont rien à voir avec "posséder XXX millions" ou faire partie des méga-riches. Donc, je vais faire quelque chose d'autre : donner la majorité de mes bitcoins à des œuvres de charité. J'appellerai ça le "Pineapple Fund". Oui, je donne environ 86 millions de dollars de bitcoin à des œuvres caritatives. »[1] Ce donateur a choisi de ne pas révéler son identité, « Le Pinneaple Project n'est pas une affaire de publicité » affirme-t-il. Chacun peut aller sur son site (pineapplefund.org) et lui conseiller des associations à aider, c'est aussi ça « l'effet réseau ».

1. « Appel à conseil d'un redditeur : à quelle œuvre donner 5 057 BTC ? » journalducoin.com, 16 décembre 2017.

© Groupe Eyrolles